

10/540e33

PCT/JPC3/16538

日本国特許庁  
JAPAN PATENT OFFICE

24.12.03

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日  
Date of Application: 2002年12月24日

出願番号  
Application Number: 特願2002-371448

[ST. 10/C]: [JP2002-371448]

出願人  
Applicant(s): 福嶋 一

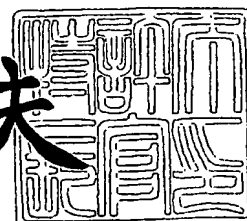
REC'D 19 FEB 2004	
WIPO	PCT

PRIORITY DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH  
RULE 17.1(a) OR (b)

2004年 2月 5日

特許庁長官  
Commissioner,  
Japan Patent Office

今井康夫



BEST AVAILABLE COPY

【書類名】 特許願

【整理番号】 P021224NSC

【あて先】 特許庁長官殿

【発明者】

    【住所又は居所】 東京都中野区野方二丁目 6 2 番 3 号

    【氏名】 福島 一

【特許出願人】

    【識別番号】 300062120

    【氏名又は名称】 有限会社グルーネット

    【代表者】 福島 一

【特許出願人】

    【識別番号】 301047980

    【氏名又は名称】 福島 一

【手数料の表示】

    【予納台帳番号】 111672

    【納付金額】 21,000円

【提出物件の目録】

    【物件名】 明細書 1

    【物件名】 図面 1

    【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 動的 IP アドレス割当てを受けた機器を管理する方法およびシステム

【特許請求の範囲】

【請求項 1】 TCP/IP ネットワークにおいて、  
ドメイン名に対するホスト名の IP アドレスを動的に更新するシステムにおいて、

IP アドレスの割当てを動的に受けてなる計算機もしくはネットワーク接続機器を管理対象機器 (4100) とする場合か、

IP アドレスの割当てを動的に受けてなる装置と一体となって外部ネットワークから参照される計算機もしくはネットワーク接続機器もしくはシステムを管理対象機器 (4100) とする場合であって、

管理サーバ (2000) と管理対象機器 (4100) とが所定の通信をすることによって、管理対象機器 (4100) の真性を管理サーバ (2000) に確認させることを特徴とするネットワーク管理の方法。

【請求項 2】 TCP/IP ネットワークにおいて、  
ドメイン名に対するホスト名の IP アドレスを動的に更新するシステムにおいて、

IP アドレスの割当てを動的に受けてなる計算機もしくは IP アドレスの割当てを動的に受けてなるネットワーク接続機器か、

あるいは IP アドレスの割当てを動的に受けたネットワーク境界を構成する機器と一体となって参照される計算機もしくはネットワーク接続機器もしくはシステムのいずれかを管理対象機器 (4100) とする場合であって、

管理対象機器 (4100) を管理するための計算機であるところの管理サーバ (2000) から管理対象機器 (4100) に対して所定の方式での通信をサインとして送信し、

前記サインに対して管理対象機器 (4100) は所定のカウンターサインを返信するという、

サイン・アンド・カウンターサインをもって、

管理サーバ (2000) が管理対象機器 (4100) をその他のホストと誤認されておらず真性の管理対象機器 (4100) であることを確認することを特徴とするネットワーク管理の方法。

【請求項 3】 TCP/IP ネットワークにおいて、

ドメイン名に対するホスト名の IP アドレスを動的に更新するシステムにおいて、

ネットワーク境界を構成する装置の少なくとも 1 のインターフェースの IP アドレスの割当てが変化する場合であって、

管理サーバ (2000) において、管理対象機器 (4100) 毎にあらかじめ合意された通信の方式と合意された方式での通信に対する答えられるべき返事の組あるいはペアテーブルを作成し、これを管理サーバ (2000) に設定し、

カスタマネットワーク上のサーバもしくは端末機器などの計算機あるいはルータなどの複数のノードを有するネットワーク境界を構成するゲートウェイ装置もしくはプロトコル変換をする装置などのネットワーク接続機器を含む IP アドレスの割当てを動的に受けてなる装置か、あるいは該装置に静的 NAT もしくはポートフォワーディングなどが設定されることによって外部ネットワークからは該装置と一体となって参照される計算機もしくはネットワーク接続機器もしくはシステムのいずれかであるところの管理対象機器 (4100) にあらかじめ合意された方式での通信に対する答えられるべき返事を設定し、

管理サーバ (2000) から、管理対象機器 (4100) に対してあらかじめ合意された方式での通信を行ない、管理対象機器 (4100) からの返事が、管理対象機器 (4100) から答えられるべき返事であった場合に、

管理対象機器 (4100) が正常に稼動するか真性なホストであることを確認することを特徴とするネットワーク管理の方法。

あるいは、管理対象機器 (4100) からの返事が答えられるべき返事でなかった場合か返事がなかった場合に、管理対象機器 (4100) が正常に稼動しないか真性なホストでないことを確認することを特徴とするネットワーク管理の方法。

【請求項 4】 請求項 3 に記載のネットワーク管理方法において、あらかじめ合意された通信の方式として、管理対象機器 (4100) において待受けするポー

トに S N M P ( R F C 1 7 0 0 A S S I G N E D N U M B E R S でいうところの S N M P と同じか類似するもの) を用いることを特徴とするネットワーク管理の方法。

【請求項 5】 請求項 3 に記載のネットワーク管理方法において、あらかじめ合意された通信の方式として、管理対象機器 (4100) において待受けするポートに D O M A I N ( R F C 1 7 0 0 A S S I G N E D N U M B E R S でいうところの D O M A I N と同じか類似するもの) を用いることを特徴とするネットワーク管理の方法。

【請求項 6】 請求項 3 に記載のネットワーク管理方法において、あらかじめ合意された通信の方式として、管理対象機器 (4100) において待受けするポートに S M T P ( R F C 1 7 0 0 A S S I G N E D N U M B E R S でいうところの S M T P と同じか類似するもの) を用いることを特徴とするネットワーク管理の方法。

【請求項 7】 請求項 3 に記載のネットワーク管理方法において、あらかじめ合意された通信の方式として、管理対象機器 (4100) において待受けするポートに H T T P ( R F C 1 7 0 0 A S S I G N E D N U M B E R S でいうところの w w w - h t t p や h t t p s と同じか類似するもの) を用いることを特徴とするネットワーク管理の方法。

【請求項 8】 請求項 3 に記載のネットワーク管理方法において、管理対象機器 (4100) において、管理対象機器 (4100) の記憶装置に所定の値あるいは文字列を答えるべき返事として保存し、あらかじめ合意された所定の方式での通信に対して前記保存された値あるいは文字列を記憶装置より読み出し、少なくとも該値あるいは該文字列を含めた返事を返信することを特徴とするネットワーク管理の方法。

【請求項 9】 請求項 2 あるいは請求項 3 のいずれかに記載のネットワーク管理方法に先だて、管理対象機器 (4100) のドメインを管理する D N S サーバを正引き名前問合せをして直接に管理対象機器 (4100) の I P アドレスを得て、請求項 2 あるいは請求項 3 のいずれかに記載の管理対象機器 (4100) と通信するために上で得た I P アドレスを用いておこなうことを特徴とするネットワーク管理の方法。

【請求項 1 0】 S N M P マネージャを用いてする (トラフィックや負荷率

などを対象とするなどの) 従来のネットワーク管理の方法に先だって、請求項 2 もしくは請求項 3 に記載の管理対象機器 (4100) の真性確認を実施し、ここで管理対象機器 (4100) が真性であることが確認された場合に、真性であることが確認されたネットワーク上で管理対象機器 (4100) を特定する情報を用いて、従来のネットワーク管理の方法で動的に IP アドレスが変化する管理対象機器 (4100) を管理することを特徴とするネットワーク管理の方法。

【請求項 1 1】 請求項 2 あるいは請求項 3 のいずれかに記載のネットワーク管理方法において、

管理対象機器 (4100) の真性確認に失敗した場合に、所定の時間間隔を経過した後、再度請求項 2 ないし請求項 3 に記載のネットワーク管理方法を実施することによって、管理対象機器 (4100) に障害が発生していることを確認するか、管理対象機器 (4100) に到達する経路上のネットワークの都合によって管理対象機器 (4100) が見失われていることを確認することを特徴とするネットワーク管理の方法。

【請求項 1 2】 管理対象機器 (4100) を管理するためのシステムであって、該システムに管理対象機器 (4100) 毎に少なくともサインとカウンターサインが設定され、該システムから管理対象機器 (4100) にサインを送信するステップと、管理対象機器 (4100) から返信されるカウンターサインを受信するステップと、前記受信されたカウンターサインと前記設定されたカウンターサインとを照合するステップとを備え、照合された結果が真であることによって管理対象機器 (4100) が真性の管理対象機器 (4100) であることを確認することを特徴とするシステム。

【請求項 1 3】 管理対象機器 (4100) を管理するためのシステムであって、該システムに管理対象機器 (4100) 毎に少なくともあらかじめ合意された通信の方式と合意された方式での通信に対する答えられるべき返事の組あるいはペーテーブルが設定され、該システムからあらかじめ合意された通信の方式で管理対象機器 (4100) に問い合わせるステップと、管理対象機器 (4100) からの返事を受信するステップと、前記受信された返事と前記設定された合意された方式での通信に対する答えられるべき返事とを照合するステップとを備え、照合された結

果が真であることによって管理対象機器 (4100) が真性の管理対象機器 (4100) であることを確認することを特徴とするシステム。

【請求項 14】 請求項 12 あるいは請求項 13 のいずれかに記載の処理に先だって、管理対象機器 (4100) のホスト名を含むドメインを管理する DNS サーバを正引き名前問合せをして直接に管理対象機器 (4100) の IP アドレスを得て、請求項 12 あるいは請求項 13 のいずれかに記載の管理対象機器 (4100) と通信するために上で得た IP アドレスを用いておこなうことを特徴とするシステム。

【請求項 15】 請求項 12 あるいは請求項 13 のいずれかに記載の処理に後続して、SNMP マネージャを用いてする (トラフィックや負荷率などを対象とするなどの) 従来のネットワーク管理の方法に接続するために、

請求項 12 もしくは請求項 13 に記載された真性であることが確認されたネットワーク上で管理対象機器 (4100) を特定する情報を用いて、従来のネットワーク管理の方法で動的に IP アドレスが変化する管理対象機器 (4100) を管理することを特徴とするシステム。

【請求項 16】 請求項 12 あるいは請求項 13 のいずれかに記載のシステムであって、

管理対象機器 (4100) の真性確認に失敗した場合に、所定の時間間隔を経過した後、再度請求項 12 ないし請求項 13 に記載の処理を実施することによって、管理対象機器 (4100) に障害が発生していることを確認するか、管理対象機器 (4100) に到達する経路上のネットワークの都合によって管理対象機器 (4100) が見失われていることを確認することを特徴とするシステム。

【請求項 17】 計算機もしくはネットワーク接続機器にあって IP アドレスの割当てを動的に受けてなる装置か、

あるいは外部ネットワークからは該装置と一体となって参照される計算機もしくはネットワーク接続機器もしくはシステムのいずれかにあって、

該計算機もしくは該ネットワーク接続機器もしくは該システムの記憶装置に任意の値もしくは文字列をカウンターサインもしくは答えるべき返事として保存し、サインもしくはあらかじめ合意された任意の方式での通信に対して前記保存さ

れた値もしくは文字列を記憶装置より読み出し、少なくとも該値もしくは該文字列を含めたカウンターサインもしくはあらかじめ合意された方式での通信に対する返事を返信するように構成されることを特徴とする計算機もしくはネットワーク接続機器もしくはシステム。

【請求項 18】 請求項 17 に記載の計算機もしくはネットワーク接続機器もしくはシステムにおいて、

該計算機もしくは該ネットワーク接続機器もしくは該システムにはホスト名が設定されるものであって、該ホスト名が該計算機もしくは該ネットワーク接続機器もしくは該システムの記憶装置に保存され、H T T P（もしくは類似の）ポートへの通信要求を受けた際に、前記保存されたホスト名を該記憶装置より読み出し、少なくとも該ホスト名を含めた文字列を返信するように構成されることを特徴とするか前記手順を備えることを特徴とする計算機もしくはネットワーク接続機器もしくはシステム。

【請求項 19】 請求項 17 に記載の計算機もしくはネットワーク接続機器もしくはシステムにおいて、

ダイナミック DNS によって動的更新されるセンタ側 DNS サーバ (1000) において設定されるホスト名が F Q D N でもって、該計算機もしくは該ネットワーク接続機器もしくは該システムのホスト名として設定されるものであって、該ホスト名が該計算機もしくは該ネットワーク接続機器もしくは該システムの記憶装置に保存され、H T T P（もしくは類似の）ポートへの通信要求を受けた際に、前記保存されたホスト名を該記憶装置より読み出し、少なくとも該ホスト名を含めた文字列を返信するように構成されることを特徴とするか前記手順を備えることを特徴とする計算機もしくはネットワーク接続機器もしくはシステム。

【請求項 20】 請求項 17 に記載の計算機もしくはネットワーク接続機器もしくはシステムにおいて、

ダイナミック DNS によって動的更新されるセンタ側 DNS サーバ (1000) において設定されるホスト名を F Q D N でもって、該計算機もしくは該ネットワーク接続機器もしくは該システムに読み出し可能な文字列として設定されるものであって、該文字列が該計算機もしくは該ネットワーク接続機器もしくは該システ



ムの記憶装置に保存され、H T T P（もしくは類似の）ポートへの通信要求を受けた際に、前記保存された文字列を該記憶装置より読み出し、少なくとも該文字列を含めた文字列を返信するように構成されることを特徴とするか前記手順を備えることを特徴とする計算機もしくはネットワーク接続機器もしくはシステム。

【請求項 2 1】 請求項 1 8 ないしは請求項 2 0 のいずれかに記載の計算機もしくはネットワーク接続機器もしくはシステムにおいて、

請求項 1 8 ないしは請求項 2 0 のいずれかに記載の待受けされる H T T P（もしくは類似の）ポート以外に、該計算機もしくは該ネットワーク接続機器もしくは該システムの設定変更用のポートあるいは、一般の閲覧に供するためのウェブサービスを提供するウェルノウンなポート（ポートフォワーディングなどをするために設定される場合を含む）のいずれかのポート、あるいはその両方のポートで待受けされる H T T P（もしくは類似の）ポートを備えるように構成されることを特徴とするか前記手順を備えることを特徴とする計算機もしくはネットワーク接続機器もしくはシステム。

【請求項 2 2】 請求項 1 7 に記載のネットワーク接続機器において、

前記ネットワーク接続機器が S N M P エージェントを実装したネットワーク接続機器である場合であって、

あらかじめ合意された通信の方式として、S N M P（R F C 1 7 0 0 ASSIGNED NUMBERS でいうところの S N M P と同じか類似するもの）を用いる場合でかつ返事に S N M P におけるオブジェクト I D を用いる場合には、S N M P エージェントを実装したネットワーク接続機器を除くが、

あらかじめ合意された通信の方式として、S N M P を用いない場合には、S N M P エージェントを実装したネットワーク接続機器を含めることを特徴とするネットワーク接続機器。

【請求項 2 3】 計算機もしくはネットワーク接続機器にあって I P アドレスの割当てを動的に受けてなる装置か、

あるいは外部ネットワークからは該装置と一体となって参照される計算機もしくはネットワーク接続機器もしくはシステムのいずれかにあって、

該計算機もしくは該ネットワーク接続機器もしくは該システムに着脱自在に設

けられた外部記憶媒体であって、

サインもしくはあらかじめ合意された任意の方式での通信に対して、カウンターサインもしくは答えるべき返事として読み出すための任意の値もしくは文字列を格納したことを特徴とする記録媒体か、

あるいは、サインもしくはあらかじめ合意された任意の方式での通信に対して、前記格納された任意の値もしくは文字列を読み出し、少なくとも該値もしくは該文字列を含むカウンターサインもしくは答えるべき返事をするためのプログラムを格納したことを特徴する記録媒体。

【請求項 2 4】 管理対象機器 (4100) から管理サーバ (2000) に対して、アライブメッセージの送信をおこない、

管理サーバ (2000) では、管理対象機器 (4100) からのアライブメッセージを受信することによって管理対象機器 (4100) の I P アドレスの変化にかかわらず管理対象機器 (4100) が、どの管理対象機器 (4100) であるかを識別するかあるいは管理対象機器 (4100) が少なくとも生存していることを確認することを特徴とするネットワーク管理の方法。

【請求項 2 5】 管理対象機器 (4100) から管理サーバ (2000) に対して、アライブメッセージの送信をおこない、

管理サーバ (2000) では、管理対象機器 (4100) からの該通信を受付ける際に認証をおこなうことによって管理対象機器 (4100) の I P アドレスの変化にかかわらず管理対象機器 (4100) が、どの管理対象機器 (4100) であるかを識別するかあるいは管理対象機器 (4100) が少なくとも生存していることを確認することを特徴とするネットワーク管理の方法。

【請求項 2 6】 管理対象機器 (4100) から管理サーバ (2000) に対して、公開かぎ暗号方式を用いたアライブメッセージの送信をおこない、

管理サーバ (2000) では、管理対象機器 (4100) からのアライブメッセージの復号化をおこなうことによって管理対象機器 (4100) の I P アドレスの変化にかかわらず管理対象機器 (4100) が、どの管理対象機器 (4100) であるかを識別するかあるいは管理対象機器 (4100) が少なくとも生存していることを確認することを特徴とするネットワーク管理の方法。

【請求項 2 7】 請求項 2 4 ないしは請求項 2 6 に記載のいずれかのネットワーク管理方法において、

管理対象機器 (4100) から管理サーバ (2000) へのアライブメッセージの送信は、所定の時間間隔でおこなわれるものとし、

管理サーバ (2000) ではアライブメッセージの所定の時間間隔での到着が途切れたことをもって管理対象機器 (4100) に障害が発生したことを検出することを特徴とするネットワーク管理の方法。

【請求項 2 8】 請求項 2 7 に記載のネットワーク管理方法において、

管理対象機器 (4100) から管理サーバ (2000) へ所定の時間間隔でおこなわれるアライブメッセージの送信間隔と、

管理サーバ (2000) でアライブメッセージの所定の時間間隔での到着をチェックする処理の実行間隔が、同一の時間間隔であることを特徴とするネットワーク管理の方法。

【請求項 2 9】 管理対象機器 (4100) からのアライブメッセージを受信することによって管理対象機器 (4100) の IP アドレスの変化にかかわらず管理対象機器 (4100) が、どの管理対象機器 (4100) であるかを識別するかあるいは管理対象機器 (4100) が少なくとも生存していることを確認することを特徴とするシステム。

【請求項 3 0】 管理対象機器 (4100) からのアライブメッセージを受付ける際に認証をおこなうことによって管理対象機器 (4100) の IP アドレスの変化にかかわらず管理対象機器 (4100) が、どの管理対象機器 (4100) であるかを識別するかあるいは管理対象機器 (4100) が少なくとも生存していることを確認することを特徴とするシステム。

【請求項 3 1】 管理対象機器 (4100) から送信された公開かぎ暗号方式を用いて暗号化されたアライブメッセージの復号化をおこなうことによって管理対象機器 (4100) の IP アドレスの変化にかかわらず管理対象機器 (4100) が、どの管理対象機器 (4100) であるかを識別するかあるいは管理対象機器 (4100) が少なくとも生存していることを確認することを特徴とするシステム。

【請求項 3 2】 請求項 2 9 ないしは請求項 3 1 に記載のいずれかのシステ

ムにおいて、

アライブメッセージが所定の時間間隔で到着する場合において、このアライブメッセージの到着が途切れたことをもって管理対象機器（4100）に障害が発生したことを検出することを特徴とするシステム。

【請求項 3 3】 請求項 3 2 に記載のシステムにおいて、

管理対象機器（4100）からの予定されたアライブメッセージの到着間隔で、アライブメッセージの到着をチェックする処理を実行することを特徴とするシステム。

【請求項 3 4】 管理サーバ（2000）に対して、アライブメッセージを送信することをもって、管理対象機器（4100）の IP アドレスを管理サーバ（2000）に知らせるか、あるいは管理対象機器（4100）の生存を管理サーバ（2000）に確認させることを特徴とする計算機もしくはネットワーク接続機器もしくはシステム。

【請求項 3 5】 管理サーバ（2000）に対して、ユーザー名およびパスワードを含むアライブメッセージを送信することをもって、管理対象機器（4100）の IP アドレスを管理サーバ（2000）に知らせるか、あるいは管理対象機器（4100）の生存を管理サーバ（2000）に確認させることを特徴とする計算機もしくはネットワーク接続機器もしくはシステム。

【請求項 3 6】 管理サーバ（2000）に対して、管理サーバ（2000）の公開かぎで暗号化したアライブメッセージを送信することをもって、管理対象機器（4100）の IP アドレスを管理サーバ（2000）に知らせるか、あるいは管理対象機器（4100）の生存を管理サーバ（2000）に確認させることを特徴とする計算機もしくはネットワーク接続機器もしくはシステム。

【請求項 3 7】 請求項 3 4 ないしは請求項 3 6 に記載のいずれかの計算機もしくはネットワーク接続機器において、

管理サーバ（2000）に対するアライブメッセージの送信が、所定の時間間隔でおこなわれることを特徴とする計算機もしくはネットワーク接続機器もしくはシステム。

【請求項 3 8】 計算機もしくはネットワーク接続機器にあって IP アドレ

スの割当てを動的に受けてなる装置か、

あるいは外部ネットワークからは該装置と一体となって参照される計算機もしくはネットワーク接続機器もしくはシステムのいずれかにあって、

該計算機もしくは該ネットワーク接続機器もしくは該システムに着脱自在に設けられた外部記憶媒体であって、

該計算機もしくは該ネットワーク接続機器の管理を管理サーバ (2000) にさせるために、

アライブメッセージを送信するための任意の値もしくは文字列、ユーザー名とパスワードあるいは管理サーバ (2000) の公開かぎを格納したことを特徴とする記録媒体か、

あるいは、前記格納された任意の値もしくは文字列、ユーザー名とパスワードを読み出し、該値もしくは該文字列を管理サーバ (2000) の公開かぎで暗号化するプログラムを格納するか、少なくとも該値もしくは該文字列もしくは該ユーザー名と該パスワードもしくは前記管理サーバ (2000) の公開かぎでされた暗号を管理サーバ (2000) に送信するプログラムを格納したことを特徴する記録媒体。

【請求項 3 9】 請求項 2 4 ないしは請求項 2 8 に記載のいずれかのネットワーク管理方法において、

管理サーバ (2000) では認証に失敗したこともしくはアライブメッセージの到着が途切れたことをトリガとして、請求項 2 あるいは請求項 3 のいずれかに記載のネットワーク管理の方法を実施することを特徴とするネットワーク管理の方法。

#### 【発明の詳細な説明】

##### 【0 0 0 1】

#### 【発明の属する技術分野】

本発明は TCP / IP におけるネットワーク管理技術に属する。

TCP / IP ネットワークにおいて固定的な IP アドレスの割当てを受けない (動的割当てを受けた) ホストで TCP / IP によるネットワークサービス (以下、「インターネットサービス」とする。なお、ここでは TCP / IP によるネット

ワークサービスでありさえすれば、広域のインターネットワーキング（以下、「グローバルサービス」とする）であるか任意の範囲で閉じたネットワーク（通常「イントラネット」あるいは「ローカルエリアネットワーク」（以下、「LAN」とする）などと呼ばれている）であるかを問わないものとする）を提供させる際の管理技術に属する。

#### 【0002】

##### 【従来の技術】

インターネット(=the Internet)は非常に多数のコンピュータとコンピュータ・ネットワークから構成され、これらはTCP/IPプロトコルを用いた通信リンクを通して世界的な規模で相互に接続されている。相互に接続されたコンピュータは、電子メール、ゴーファー、およびワールドワイドウェブなどの、様々なインターネットサービスを利用して情報をやりとりしている。

#### 【0003】

インターネットは、ネットワーク割当て団体から一意に割当てられたIPアドレスによって、そのホストを識別している。IPアドレスは、計算機が処理し易いように固定長の数字の羅列として表現されており、人間にとっては無意味綴りであり、覚えたり毎回間違えずに入力したりするのが困難である。TCP/IPネットワークにおいては、ホストを特定するためには少なくともIPアドレスが必要であり、IPアドレスでホストを特定することが人間にとって判りにくいものであるという問題を軽減するために、ドメインネームシステム（以下、「DNS」とする）を用いてホストを特定することがおこなわれてきた。

#### 【0004】

DNSは、IPアドレスのような数字の羅列ではなく、人間にとって意味がある文字列でインターネット上のホストを特定するためのデータベースシステムである。図2に示すように階層的な名前空間を構成しており、ドメイン名と呼ばれる文字列を登録しておき、これをIPアドレスと対応づけることによって、インターネット上のホストを特定する。これを正引き名前解決という。逆に、IPアドレスからドメイン名を検索することを逆引き名前解決という。DNSの特徴は、ルートサーバを頂点とする木構造の分散データベースである。また、IPアド

レスはルーティングの制約を受けるが、DNSにおける名前はホストのネットワーク的な位置とは無関係に存在できる。

#### 【0005】

一般にインターネットに常時接続し、IPアドレスの割当てを受けた各利用組織は、ドメイン名の登録団体に対して、ドメインの登録をおこない、自組織のためのドメイン名の運用をおこなう。この時にドメイン運用をおこなうサーバがDNSサーバである。なお、DNSサーバの登録には、ドメイン名の登録団体に対してIPアドレスおよびホスト名を指定して、DNSサーバの登録をおこなう。

#### 【0006】

ルートサーバは第一レベルのDNSサーバに、第一レベルのDNSサーバは第二レベルのDNSサーバに、そして最終的に上で示したIPアドレスの割当てを受けた各利用組織のDNSサーバにドメイン運用の権限の委譲をおこなう。図19に、DNSの検索順を示す。IPアドレスの割当てを受けた各利用組織のDNSサーバでは、ドメイン名に対するホスト名とIPアドレスの対応づけや、メールの配送経路の指定などといった実際の設定をおこなう。

#### 【0007】

旧来DNSは設定ファイルを手動で設定および更新されてきた。ところが主に社内で利用されるプライベートLANなどにおいて、Windows（登録商標、以下同様）パソコンの普及とダイナミック・ホスト・コンフィグレーション・プロトコル（DHCP）による端末となるパソコンの動的なネットワーク設定の普及によって、Windowsパソコンが再起動されるたびにIPアドレスが変化するなどの、従来のように静的に1のホスト名と1のIPアドレスを対応づけることが難しくなってきた。ダイナミックDNSとは、DNSサーバのレコードの更新をクライアントからのアップデート要求によって自動的に更新するしくみを提供するものである。ダイナミックDNSの利用について、社内LANなどの直接インターネットに接しないネットワークにおける利用だけではなく、インターネットのグローバルサービスの中でも、現在、実用性の検証がされている。

#### 【0008】

インターネットのグローバルサービスの中でダイナミックDNSサービスを利

用した場合には、ネットワーク割当て団体からネットワークの割当てを受けないあるいはプロバイダから固定的な IP アドレス割当てを受けない(ダイヤルアップの)ホストで、インターネットサービスを提供することが出来るようになる。

#### 【0009】

ところで、ダイヤルアップとは、主にダイヤルアップ接続としてインターネットに接続する際に電話をかける行為を伴うものをいうが、近年ケーブルテレビやデジタル加入者回線、光ファイバをアクセス回線に用いた定額制の IP 接続役務などによるアクセス回線の多様化により、必ずしも電話をかける行為を必要としなくなっている。これら近年の常時接続型と呼ばれるインターネット接続役務は、単に接続時間による課金体系でなくなったことを意味し、ルータのセッション異常終了(停電など)、回線の異常、センタの故障やメンテナンスなどにより接続が異常切断された場合や接続業者もしくはダイヤルアップするホストの無通信タイマーによって回線が切断された場合などに再接続すると、IP アドレスが変わる場合があるという点で専用線による接続と異なる。そこで本発明では、従来の専用線による接続に代表されるネットワーク割当て団体から恒常的なネットワークの割当てを受けて接続する場合かプロバイダ(あるいは IP アドレスの割当てを受けた各利用組織)から恒常的な IP アドレスの割当てを受けて接続する場合と対比して、プロバイダ(あるいは IP アドレスの割当てを受けた各利用組織)からの一時的な利用を前提とした IP アドレスの割当てを受けて接続することを(モデムを用いて電話をかけるという行為を伴わず、DHCP や PPPoE などによる割当てであったとしても)「ダイヤルアップ接続」といい、一時的な IP アドレスの割当てを受けるための動作をすることを「ダイヤルアップする」という。また、IP アドレスの一時的な割当てそのものを「ダイヤルアップ」ということとする。

#### 【0010】

##### 【ダイナミック DNS 特有の問題】

従来の技術では、IP アドレスが変化するホストでのインターネットサービスの提供はできなかったが、ごく最近になってダイナミック DNS を用いることによって、限定的に(グローバルサービスとしての DNS は固定 IP アドレスが必



要なことからDNS以外の) インターネットサービスを提供できるようになった。しかし、ダイナミックDNSを用いることに特有の以下の問題点があったので、これを以下の図で説明する。

図3。管理対象機器(4100)からプロバイダA(4000)へダイヤルアップ(PPPoEなどを含む)する。

図4。管理対象機器(4100)はプロバイダA(4000)からIPアドレスの動的割当てを受ける。この時、割当てを受けたIPアドレスを仮に172.16.100.100とする。

図5。管理対象機器(4100)はセンタ側DNSサーバ(1000)へDNSの更新要求をし、ダイナミックDNSを運用するセンタ側のDNSサーバ(1000)(以下、「センタ側DNSサーバ」とする)は図4で管理対象機器(4100)に割当てられたIPアドレス(仮に172.16.100.100)をDNSに設定する。

図6。管理対象機器(4100)は、インターネットの一般利用者(5300)からのアクセスを受ける事ができる(正常状態)。

図7。なんらかの理由で管理対象機器(4100)からプロバイダA(4000)への接続が失われるなどの障害が発生する。

#### 【0011】

図8。管理対象機器(4100)からプロバイダA(4000)へ再接続(PPPoEなどを含む)する。

図9。管理対象機器(4100)はプロバイダA(4000)からIPアドレスの動的割当てを受ける。IPアドレスが変化するまで割当てられていたIPアドレス(仮に172.16.100.100)とは別のIPアドレス(仮に172.16.200.10)が割当てられる。

図10。管理対象機器(4100)はセンタ側DNSサーバ(1000)へDNSの更新要求をだし、センタ側DNSサーバ(1000)は図9で割当てられたIPアドレス(仮に172.16.200.10)をDNSに設定する。

#### 【0012】

図11。図9において、この時、管理対象機器(4100)のIPアドレスはIPアドレスが変化するまで割当てられていたIPアドレスとは別のアドレス(仮に

172.16.200.10) を割当てられており、管理対象機器 (4100) に IP アドレスが変化するまで割当てられていた IP アドレス (仮に 172.16.100.100) は同一プロバイダの別のユーザ (4200) に割当てられている。この場合において、インターネットの一般利用者 (5300) から見るとホストがすり替わっているかのように見える。

図 12。インターネット全体では参照される DNS はここでいうセンタ側 DNS サーバ (1000) ではあり得ず、各利用者毎に直接接続されたプロバイダの DNS (4500 や 5500 など) である事がほとんどであると思われる。そのため、仮にセンタ側 DNS サーバ (1000) が正常に更新されたとしても、キャッシュの生存時間内には、各利用者毎に直接接続されたプロバイダの DNS (4500 や 5500 など) からセンタ側 DNS サーバ (1000) への名前問合せは行われないうちに、これらの DNS サーバに管理対象機器 (4100) の IP アドレス (仮に 172.16.200.10) が反映されるには時間がかかる。

#### 【0013】

DNS (4500 や 5500 など) は、一度問合せをおこなったリソースレコードに関して、一定期間ローカルに記憶しておく。これをキャッシュという。キャッシュは、リソースレコードの TTL (=time to live。キャッシュの生存時間に同じ) で指定された期間だけ記憶され、その後破棄される。これをキャッシュの生存時間という。キャッシュの生存時間中は、DNS (4500 や 5500 など) はリゾルバ (4100 や 4200 あるいは 5300 など) からの問合せに対して、ローカルな記憶を参照して名前解決するために、一度おこなった名前問合せを繰り返すことを抑制し、効率をよくするために考えられた。しかし、ダイナミック DNS においては、このキャッシュというメカニズムが逆に管理対象機器 (4100) の IP アドレスの変化に追従できないなどのうまく合致していない部分があるので、以下に説明する。

#### 【0014】

図 18 に、一般利用者 (5300) からどのように DNS が探索され、目的ホストである管理対象機器 (4100) に到達するかを順に見てみる。

①で、一般利用者 (5300) からプロバイダ B の DNS (5500) へ、管理対象機

器 (4100) について正引き名前問合せをおこなう。

②、プロバイダBのDNS (5500) は、まず、目的ドメイン名を知っているかどうかを調べ、知っている場合は、即座に目的ホストである管理対象機器 (4100) のIPアドレスを一般利用者 (5300) に返す。この時、プロバイダBのDNS (5500) が目的ドメイン名を知っている場合とは、目的ドメイン名をプロバイダBのDNS (5500) が運用している場合と、目的ホストである管理対象機器 (4100) に対するIPアドレスがプロバイダBのDNS (5500) に、キャッシュされている場合である。プロバイダBのDNS (5500) が目的ドメイン名を知らない場合を、図19に示す。

③、②によって管理対象機器 (4100) のIPアドレスを知ることができた一般利用者 (5300) は、これをもとに、管理対象機器 (4100) へアクセスする。

#### 【0015】

図19は、図18の②で、プロバイダBのDNS (5500) が管理対象機器 (4100) のドメインを運用していない場合と、キャッシュされていない場合 (最初の名前問合せの時) のDNSの探索順である。

①で、一般利用者 (5300) からプロバイダBのDNS (5500) へ、管理対象機器 (4100) について正引き名前問合せをおこなう。

②、プロバイダBのDNS (5500) は、目的ドメイン名である管理対象機器 (4100) のドメインを運用しておらず、キャッシュの中からも見つけられなかった場合、Root DNSに、名前問合せをする。

③、Root DNSは、仮に目的ホストである管理対象機器 (4100) のドメイン名が例としてJPドメインであった場合には、JP DNSの所在を返す。

(管理対象機器 (4100) のドメイン名がJPドメインではない場合には、ccTLDなり、gTLDなりを管理するネームサーバの所在をプロバイダBのDNS (5500) に返す。)

④、プロバイダBのDNS (5500) は、③で得たJPドメインのDNSに対して、目的ドメイン名である管理対象機器 (4100) のドメインを名前問合せをする。

。

⑤、JPドメインのDNSは、目的ホストである管理対象機器 (4100) のドメ

イン名を運用するサーバ（ここではセンタ側DNSサーバ（1000））の所在を（JP配下のドメインは、JPNICおよび会員のサーバに登録されるツリー構造であり、第二レベル毎のDNSには分かれていないため、すぐに）プロバイダBのDNS（5500）に返す。

⑥、プロバイダBのDNS（5500）は、⑤で得たセンタ側DNSサーバ（1000）に対して、管理対象機器（4100）のIPアドレスを名前問合せをする。

⑦、センタ側DNSサーバ（1000）は、管理対象機器（4100）の所在をプロバイダBのDNS（5500）に返す。

⑧、プロバイダBのDNS（5500）は、⑦で得た管理対象機器（4100）の所在を一般利用者（5300）に返す。

⑨、一般利用者（5300）は、管理対象機器（4100）へアクセスする。

図20。DNS（4500や5500など）は、最初の名前問合せによってキャッシュされ、その後キャッシュの期限が過ぎた事によって、キャッシュが無効となるよう設定するのが一般的である。このキャッシュが無効なタイミング（図19）では、センタ側DNSサーバ（1000）に対して名前問合せがおこなわれるために正しく管理対象機器（4100）のIPアドレスが得られる。しかし、キャッシュが有効な間（図18）に管理対象機器（4100）のIPアドレスが変わってしまった場合、センタ側DNSサーバ（1000）に対する名前問合せなしにキャッシュされたIPアドレスが返されるために、図10での更新より以前の（キャッシュされた）IPアドレス（仮に172.16.100.100）が返される。なお、図18の②のとおり、一般利用者（5300）の接続先であるプロバイダBのDNS（5500）が管理対象機器（4100）のドメインを運用している場合には、キャッシュの問題は発生しない。

#### 【0016】

図13。そのために、インターネット全体から見れば、このタイミングで、同一プロバイダの別のユーザ（4200）が管理対象機器（4100）として誤認されてしまうおそれがある。

またこの時、管理対象機器（4100）はメールサーバやwwwサーバの機能が設定されたホストであるものとしても、別のホスト（4200）はメールサーバやwww

wサーバの設定はされていないホストであるか、仮に設定されていたとしても管理対象機器（4100）の設定とは違う内容であるために、一般利用者（5300）からは、管理対象機器（4100）が正常でない状態（障害発生中）にあるように見えてしまう。

図14。この問題は、インターネット上の各プロバイダのDNS（4500や5500など）が、キャッシュの生存時間が過ぎ、センタ側DNSサーバに再度、名前問合せをおこなえば、収束される問題である。そのために、時間が経過するにしたがって、図14のような正常な状態となる。

#### 【0017】

次に、回線断後、管理対象機器（4100）が再接続しない（回線断のままの）場合について考えてみる。

この場合に、考えられる理由は回線障害や（ダイヤルアップをする）プログラムの障害などである。

図3ないし図7までは、前述の説明と同じである。つぎに、

図15において、この時、管理対象機器（4100）はインターネットへ接続されていない状態のためプロバイダAは、管理対象機器（4100）にIPアドレスが変化するまで割当てられていたIPアドレス（仮に172.16.100.100）を同一プロバイダの別のユーザ（4200）がダイヤルアップした時点で、別のユーザ（4200）に割当てる。

図16。センタ側DNSサーバ（4000）に設定されている管理対象機器（4100）のIPアドレスは、更新そのものが出来ないために、切断前のIPアドレス（仮に172.16.100.100）が設定されている。そのために、やはり同一プロバイダの別のユーザ（4200）が管理対象機器（4100）と誤認されてしまう。

#### 【0018】

図21は、管理対象機器（4100）の動作フローである。ここで、破線内は、管理対象機器（4100）が影響を与える外部環境の状態である。障害が発生したタイミングによって、インターネットから見失われたり、誤認されたりする。なお、図21において、S108は管理対象機器（4100）において、検出可能なイベントであると同時に外部環境の変化でもある。

## 【 0 0 1 9 】

図 2 2 は、管理対象機器 (4100) における、管理対象機器 (4100) の状態と割当て IP アドレスの関係からの障害のパターンである。

パターン 1 は、回線断のままの場合である。管理対象機器 (4100) が回線断後再接続出来なかった場合には、回線断以前に割当てられていた IP アドレスが別のユーザ (4200) に割当てられている場合に、誤認となる。割当てられていなかった場合に、アクセス不可となる。アクセス不可とは、目的ホストである管理対象機器 (4100) に到達せずに見失われた状態である。回線断のままの場合は、DNS (4500 や 5500 など) への再更新を、管理対象機器 (4100) は当然することが出来ない。

パターン 2 は、DNS へのダイナミックアップデートに失敗した場合である。管理対象機器 (4100) のダイナミックアップデートに係る部分のプログラム障害やセンタ側 DNS サーバ (1000) の障害などによって起こる。この場合において回線は、接続されているか、切断されても再接続されているものとする。この時の動作は、パターン 1 の管理対象機器 (4100) が回線断後再接続出来なかった (回線断のまま) 場合と同様に、回線断以前に割当てられていた IP アドレスが別のユーザ (4200) に割当てられている場合に、誤認となる。割当てられていなかった場合に、アクセス不可となる。また、割当て IP アドレスが変化しなかった場合には、インターネットの一般利用者 (5300) からの通信には問題がないために、正常であるようなかのように見える。

パターン 3 は、回線断後再接続した場合である。キャッシュの生存時間の影響を受け、網掛け部分はキャッシュの生存時間の影響を受ける部分であり、それ以外は、キャッシュされていないために、名前問合せがうまく行っている場合である。ここで通信の相手方であるインターネットの一般利用者 (5300) は、地域的に広がっており、個別の各インターネットの一般利用者 (5300) が以前に名前参照したことがあるか、あればキャッシュされているほど最近の名前参照であったかによって、網掛け部分に含まれるか否かが決定される。

## 【 0 0 2 0 】

図 2 2 において、網掛け部分は、管理対象機器 (4100) が回線断後再接続し、

センタ側DNSサーバ(1000)への更新もうまく行っている場合における、管理対象機器(4100)の動作としては正常であるにも関わらず、DNS(4500や5500など)が管理対象機器(4100)のIPアドレスをキャッシュしているために、管理対象機器(4100)が一時的に障害状態にあるように見えてしまうタイミングである。

#### 【0021】

以上に、キャッシュというメカニズムが逆に管理対象機器(4100)のIPアドレスの変化に追従できないなどのうまく合致していない部分があることを説明してきた。

この問題はダイナミックDNSの仕組が旧来のDNSへの拡張であり、後付けされたものであるために、発生する。

#### 【0022】

前記した通り、旧来DNSは手動で設定および更新されていた。ダイナミックDNSを利用した場合には、管理対象機器(4100)からセンタ側DNSサーバ(1000)への更新の間隔が短い場合に、DNSを参照(正引き)して得られた管理対象機器(4100)のIPアドレスは必ずしも正しいとは言えない場合があり得ることを説明してきた。

キャッシュの生存時間経過後、センタ側DNS(1000)へ名前問合せするタイミングに比して、管理対象機器(4100)の回線断およびIPアドレス更新の間隔が短すぎると、一般利用者(5300)は常に別のホストを管理対象機器(4100)と誤認することになる。回線の不安定を原因とするこのような場合にも、DNSとしては機能することが望まれるが、ダイナミックDNSとしてはこの場合において、機能し得ず一種の障害状態とみなし得る。

#### 【0023】

これはDNSをめぐるインターネット全体の問題であり、個別の実装などによって(個々のホストが対応するだけでは)解決することができない問題である。

#### 【0024】

以上によって、一時的に動的なIPアドレスを割当てられたホストにおいては、ホストの動作としては正常であったとしても、障害状態に見えてしまうなどの

問題があり、ホストを特定しづらい状況にある。

#### 【0025】

##### 【発明が解決しようとする課題】

インターネットの一般利用者（5300）が管理対象機器（4100）だと認識していたとしても、実際には別の無関係なホストであり得る。そこで、少なくとも管理サーバ（2000）からは、管理対象機器（4100）が、誤認されたホスト（4200）でなく管理対象機器だと認識されているホストとして本当に正しい通信相手（真性なホスト）であることを確認する手段を提供する。

#### 【0026】

##### 【課題を解決するための手段】

ホストの確認については、以下の方法でもって確認する。ここでは管理サーバ（2000）から管理対象機器（4100）に対して通信をした結果から、管理対象機器（4100）が真性のホストであるかどうかの判定を、管理サーバ（2000）がする。

課題を解決するための手段は、以下の三段階でおこなう。

準備段階として、合意および設定がある。

第一の段階はアドレス確認であり、

第二の段階は真性確認である。

図27に、第一の段階および第二段階によって実際に管理対象機器（4100）の真性確認をおこなう、管理サーバ（2000）の動作を示す。

#### 【0027】

合意および設定は、準備段階である。

管理サーバ（2000）および管理対象機器（4100）の双方で、管理対象機器（4100）名に対するあらかじめ合意された通信の方式と合意された方式での通信に対する答えられるべき返事の組あるいはペアテーブルを合意する。

これを管理サーバ（2000）に設定する。

動的IPアドレスを割当てられたホストであるところのあるいは前記ホストと一体となって外部ネットワークから参照されるホストであるところの管理対象機器（4100）にあらかじめ合意された方式での通信に対する答えられるべき返事を設定する。



ただし、以上の合意および設定に先立って、管理対象機器（4100）が外部ネットワークからホスト名でアクセスできるようにするために、ドメイン名およびホスト名を選択し、センタ側DNSサーバ（1000）に登録し、管理対象機器（4100）が回線断あるいはIPアドレスの変化を検出し再接続し、DNSへの動的更新を要求するシステムなどを準備しておく。

#### 【0028】

アドレス確認は、第一の段階である。

S202において、管理サーバ（2000）からキャッシュの生存時間の問題为了避免のために、センタ側DNSサーバ（1000）に対して名前問合せ（正引き）をする。

S204において、S202の返事から管理対象機器（4100）のIPアドレスを得る。

なお、管理対象機器（4100）のIPアドレスの確認は、管理サーバ（2000）とセンタ側DNSサーバ（1000）が同一のホストである場合か管理サーバ（2000）のリゾルバがセンタ側DNSサーバ（1000）を向いている場合や、センタ側DNSサーバ（1000）のTTL（キャッシュの生存時間）の設定が極めて短い場合などは、省略することができる。

#### 【0029】

真性確認は、第二の段階である。

S202およびS204で管理対象機器（4100）のIPアドレスが得られたこの時点では、管理対象機器（4100）が正しく認識されたとおりの管理対象機器（4100）であるかどうかは、未だ確認されていない。管理対象機器（4100）とプロバイダA（4000）間の回線断やセンタ側DNS（1000）に対して管理対象機器（4100）が更新することができない場合などでは、真性確認で初めて管理対象機器（4100）が真性でないことが判明する。また、管理対象機器（4100）において提供されているサービスがあらかじめわかっていたとして、このサービスに正常にアクセスできない場合も、キャッシュの問題を除いても単にそれだけで管理対象機器（4100）がネットワークから断たれた状態にあるとは、判断できない。例えば、管理対象機器（4100）がプロバイダA（4000）に正常に接続されておりかつ

センタ側DNSサーバ(1000)への更新も正常にされている場合であって、かつキャッシュの問題も発生していない場合であってなお、サービスを提供するプログラムに障害がある場合が考えられるからである。ネットワーク管理的な考え方としては、管理対象機器(4100)がインターフェース障害や回線断などのネットワーク的な障害(根本的な障害)に陥っているのか、あるいはサービス障害(アプリケーションレベルの障害)なのかを切分けたいところである。ここで、障害切分けは低レイヤからするのが定石である。そこでこの時点では、とりあえず管理対象機器(4100)だと思われるホストに対して通信を試み、その結果から本当に管理対象機器(4100)なのかどうかを判別することによって、まずネットワーク的な障害の有無を確認することとする。

S 2 0 6において、管理サーバ(2000)からアドレス確認S 2 0 2およびS 2 0 4の結果から求められた管理対象機器(4100)のIPアドレスに対して、あらかじめ合意された方式での通信をおこなう。

S 2 0 8において、S 2 0 6の返事がなければ管理対象機器(4100)が見失われている。

S 2 1 0において、S 2 0 6の返事を受取り、この結果に対して、文字列処理をして、不要な文字列を取除いた値あるいは文字列を求める。これが管理サーバ(2000)に設定された管理対象機器(4100)からあらかじめ合意された方式での通信に対して答えられるべき返事である。

#### 【0 0 3 0】

S 2 1 2において、S 2 0 8で受取った返事を、管理サーバ(2000)に設定された、管理対象機器(4100)からの返事であるべき、あらかじめ合意された方式での通信に対する答えられるべき返事との比較をおこない、判定する。

ここで、管理対象機器(4100)が答えるべき返事と管理サーバ(2000)が受取るべき返事は同じ物であることが合意されている。

あらかじめ合意された方式での通信に対する答えられるべき返事と一致した場合は、管理対象機器(4100)は正常に動作している。

一致しない場合は、キャッシュの生存時間の問題とは無関係に、管理対象機器(4100)はインターネットに接続されていないか何らかの問題でセンタDNSに

対する更新が出来ない状態にある、との判定をおこなう。

### 【0031】

判定の結果を表示する。S 2 1 2 の判定によって、管理対象機器 (4100) が正常稼動しかつ真性な管理対象機器 (4100) であることが確認された場合 S 2 1 4 か、あるいは障害状態であることが確認された場合 S 2 1 6 とに分けられるが、この判定結果を受けてどうするかは、管理対象機器 (4100) の運用責任者と管理する側の人間との契約に基づくべきものであるため、本発明では単に結果の表示とするが、管理対象機器 (4100) が正常稼動しかつ真性の場合 S 2 1 4 では、従来は監視不可能であった IP アドレスが変化するホストに対して、トラフィック監視などの通常の監視に後続させることができるという点は特筆すべき成果である。一般的には、S 2 1 4 の場合には正常である旨のみをログに書出すなどしてあえて通知せず、管理対象機器 (4100) が正常でない状態の場合 S 2 1 6 は、アラートをあげるなどの状態を通知する処理に進むのがよい。S 2 1 6 の場合、管理対象機器 (4100) がセンタ側 DNS (1000) を更新したタイミングと重なった場合などに、センタ側 DNS (1000) が更新を反映するのに遅延が生じる可能性を考慮して、やや時間をおいて再度本プロセスを実行しそれでも障害が検出されるのを待った後、初めてアラートをあげる (S 6 0 8 に後述する) のか、あるいは誰にどのような方法でアラートをあげるのかを考慮するとよい。また、管理対象機器 (4100) が正常でない状態の場合 S 2 1 6 では、重大度に応じて、必要であれば保守および復旧段階へ移行する。

### 【0032】

この時、必要であって保守および復旧段階へ移行する場合にあって、管理対象機器 (4100) が何らかの理由でインターネットから切断された状態にある時などの管理対象機器 (4100) が発見できないかまたは、誤認されたホストのみが発見された場合においては、管理対象機器 (4100) は、管理サーバ (2000) から見失われているため、一般にアクセスするには、管理対象機器 (4100) の設置場所に行かなくてはならない。しかし、これでは障害からの迅速な復旧をはかることができないため、図 1 7 に示すように、あらかじめ第二の保守経路などを用意しておき、リモートメンテナンスできるようにしておくといよい。

## 【 0 0 3 3 】

## 【発明の実施の形態】

以下、本発明の実施の形態を図面に基づいて説明する。なお、各図面において同様の機能を有する箇所には同一の符号を付している。

## 【 0 0 3 4 】

## 実施例 1

実施例 1 は、あらかじめ合意された通信の方式に、S N M P を用いるものである。

管理対象機器 (4100) は計算機であり、直接ダイヤルアップ接続している。S N M P エージェントを実装しており、設定されているものとする。後述する図 5 0 の接続形態 1 である。

管理サーバ (2000) では、監視プログラムをタイマー実行している。

以下の件が合意され設定されているものとする。

管理サーバ (2000) には、管理対象機器 (4100) 名とあらかじめ合意された方式での通信に対する返事の組あるいはペアテーブルが作成され登録されているものとする。

S N M P などの通信の方式は、待受け側のポート番号として、以下特にことわりのない場合は、R F C 1 7 0 0 ASSIGNED NUMBERS に規定されたウェルノウン・ポートと同じか類似のものとする。R F C は、A R P A N E T 開発時代に、通信の方式を合意する (よりよくする) ために「意見を求む (=Request For Comments)」として公開された文書を起源とし、現在ではインターネットあるいは T C P / I P による通信における標準的な規約集として機能している。

S N M P (=Simple Network Management Protocol) は、けして単純とはいえない標準的なネットワーク管理用のプロトコルである。S N M P における通信ではコミュニティ名および管理対象機器 (4100) の真性確認で用いるべきオブジェクト I D を通信の方式として合意し、管理対象機器 (4100) に設定されるオブジェクト I D の値を答えられるべき返事として合意する。例としてコミュニティ名に初期値のままの P U B L I C とし、オブジェクト I D にホスト名を意味する s y s N a m e を用いる。

s y s N a m e は S N M P エージェントの設定上、ほとんどの場合で明示的に設定するものではなく、単にシステムのホスト名をそのまま引用する。ごく一部のシステムによっては F Q D N を設定できずドメイン名を含まないホスト名のみ設定できる場合があるが、ここで、管理対象機器 (4100) に設定されたホスト名は、センタ側 D N S サーバ (1000) に登録される完全修飾ドメイン名 (Fully Qualified Domain Name。ホスト名+サブドメイン名+ドメイン名からなる。以下、「F Q D N」とする) が設定されているものとする (F Q D N = 管理対象機器 (4100) 名とすることで、例を単純化できるが、F Q D N 以外 (前述のドメイン名を含まないホスト名のみである場合を含む) が設定された場合にも、以下に示すプログラム中で変数を増やすことによって対応できる (実施例 2 参照))。

ここでオブジェクト I D は、返事の内容 (= 識別子) が代入される変数だと考えればよいので、以下のようなになる。

オブジェクト I D (s y s N a m e) の値 = F Q D N = 返事の内容 = 管理対象機器名。

#### 【0035】

管理サーバ (2000) において、

1、インターネットでは U N I X (登録商標、以下同様) サーバが非常に多く使われているため、本発明実施の場合にも、U N I X 上で動作させる場合が多いだろうことが想定されること。

2、U N I X にはウェルノウンプォートなどで待受けする主要なインターネットサービスがあらかじめ導入されているか、少ない費用と労力で導入することができること。

3、U N I X には文字列処理環境が最初から O S の一部として提供されていること。

などによって、本発明部分のみの実装で実験環境が構築できることから、サンプルプログラムは U N I X 上に実装した。

W i n d o w s 系の O S の場合は、D N S については I S C 版 B I N D (最初の D N S の実装としてバークレー版 U N I X に採用されて以来、インターネットの標準 D N S である) に入替える。あるいは I S C 版 B I N D の代替物に入替え

る。代替物とは、ISC版BINDに含まれるdigコマンドのようにDNSサーバの情報を外部から精査できるものをいう。SNMPマネージャについては、マイクロソフト社製のものを採用してもよいし、OpenView（登録商標、以下同様）などの製品を新たに導入してもよい。文字列処理環境については、Windows系のOSにあっては十分にはOSに含まれていないので別途文字列処理環境を用意するか、本発明を実装する際のプログラム開発中に組み込みとした方がよいかもしれない（ただしこの場合、ISC版BINDに含まれるdigコマンドの出力に対するプログラムインターフェースの問題もあるので、いっそdigコマンド代替から作成してしまった方が、労力が少ないかもしれない）。

管理対象機器（4100）においては、Windows系のOSの場合は、Windows NTやWindows 2000にはSNMPエージェントが含まれているために、そのまま利用することができる。

以上によって、OSの種類に関わらずに、本発明を実施可能である。

#### 【0036】

管理サーバ（2000）に登録された管理対象機器（4100）名や返されるべき返事などの通信の設定に必要な項目を、図47に示す。

管理サーバ（2000）においては、通信の設定に必要な項目を設定する場合は、シーケンシャルファイルのレコードとして記憶装置に保存してもよいし、DBMSを通じてアクセスされるデータベースであっても、かまわない。また、管理対象機器（4100）毎にプログラムを用意し、そのプログラム中に設定情報を記述する方法でもよい。これらは管理サーバ（2000）において管理する管理対象機器（4100）のボリュームに応じて選択すればよい。以降の例に挙げるプログラム中に直接埋め込む方式は、管理対象機器（4100）の数が多くとも数百などの比較的小さい場合により選択である。ここで設定される内容は、管理対象機器あたりに必要な項目が含まれていればよく、付加情報が追加されていてもよい。また、項目が並ぶ順序についても図47の通りでなくても、管理対象機器（4100）あたりとして混乱のないように保存されるようにすればよい。

本発明では、記憶装置については、レジスタやキャッシュについては考慮せず、メモリおよび外部記憶装置を指すこととする。また、外部記憶装置は、管理サ

ーバ(2000)や管理対象機器(4100)の当該機器内に内蔵されるローカルな装置である必要はないものとする。例えばハードディスクドライブにおいて、ファイバーチャネルなどを経由してアクセスされるディスクアレイであっても、NFSマウントなどをされるような共有型のディスクであっても、単にハードディスクドライブとして扱う。一時記憶は、機器の再起動などの際には保持される必要がないものであり、比較的短時間で消去されるものであるが、一時記憶はメモリ上に展開されても、ハードディスクドライブなどに一時ファイルとして展開されてもよい。

管理対象機器(4100)においては、通信の設定に必要な項目は多くない。これらは、合意された方式での通信要求に応答するプログラム部分と返事そのものであるところの通信の設定に必要な項目すなわち、パラメータからなる。プログラムが実装済みであるならば、保存すべきデータ量が少ないこととなる。これらの通信の設定に必要な項目を保存する記憶装置には以下のものが考えられる。機器内の不揮発メモリ、CFカード・スマートカードなどのメモリカード類、PCMCIAインタフェースを有したハードディスクドライブか通常のハードディスクドライブ、ディスクettドライブ、MOドライブ、テープ装置などの記憶装置(か、DVD-RAMやパケットライト方式のCD-RWもしくはイメージを作成するものとしてCD-Rなどの取り外し可能な記憶媒体を利用した記憶媒体読取り装置)が利用可能であるし、書換えの頻度が極めて低い場合が考えられることから、当該機器において直接に記憶媒体に対する書換えをするのではなく交換によって保存内容の修正をおこなうCD-ROM、DVD-ROM、ROMカートリッジなどの取り外し可能な記憶媒体を利用した記憶装置まで可能である。ところで、USBインターフェースやIEEE1394インターフェースの記憶装置であっても、ハードディスクドライブにおいてSCSIインターフェースなのかIDEインターフェースなのかを区別する必要がないのと同様に、インターフェースの種類については区別する必要がない。その他にも、例えば、システムの起動時にあらかじめ指定されたホストからTFTPなどの通信を用いて、設定をロードすることも可能である。この場合の記憶装置は通信を経由した外部のホストであり、内部の記憶装置に一時記憶させることによって用いる。

これらは、実施しようとする環境（具体的な装置）にあわせて利用可能なものの中から選択すればよいものとする。

### 【0037】

図30にプログラムのサンプルを示す。本プログラムはUNIXのシェルスクリプトである。本プログラムは図27の骨格のみをプログラム化したものであり、必要最低限とした。例えば本プログラム実行時において、管理対象機器（4100）名や管理サーバ（2000）に登録された返されるべき返事をどのようにして本プログラムが得るかは、別の問題だが必須なためにプログラム中に埋め込んだ。また、後続する処理または人間によるアクションが必要な場合も、単にメッセージ出力するにとどめた。

なお、行末の矢印（-->）は表示の都合上折り返されているだけで、本当は1行であることを示している。

また、処理を示すS202などの番号は引用元の図27などから、ひきついでいる。

### 【0038】

S202およびS204はアドレス確認である。これにより、キャッシュの生存時間の問題を解決している。

キャッシュの生存時間の問題とは、DNSサーバ（4500や5500あるいは管理サーバ（2000）が参照するDNSサーバ）から管理対象機器（4100）のIPアドレスを正引き名前問合せをしようとする時に、センタ側DNSサーバ（1000）の指定したキャッシュの生存時間中の2度目以降のアクセスであって、かつ管理対象機器（4100）がその間に更新していた場合には、誤った管理対象機器（4100）のIPアドレスを得るために、管理対象機器（4100）以外のホストにアクセスしようとしてしまうことをいう。

このキャッシュの生存時間の問題を解決するために、S202では、管理サーバ（2000）からセンタ側DNSサーバ（1000）に対して名前問合せ（正引き）をしている。

図34に名前問合せの出力のサンプルを示す。下線部がセンタ側DNSサーバ（1000）に対して最後に更新された管理対象機器（4100）のIPアドレスである



。この出力結果に文字列処理を施し、下線部のみを抽出し、管理対象機器（4100）のIPアドレスを得る（S204）と、これを記憶装置に一時的に保存する。

図35に名前問合せでエラーになった場合の出力のサンプルを示す。DNSサーバが正しくない場合かDNSサーバがダウンしている場合の例である。

図36に名前問合せのエラーになった場合の出力のサンプルを示す。管理対象機器（4100）が見つからなかった場合（管理対象機器（4100）を示す情報がDNSレコード中に存在しない場合）の例である。

### 【0039】

図23ないし図26にキャッシュの生存時間のために、キャッシュされたDNS（4500で計測）を参照する場合とセンタ側DNSサーバ（1000）から直接正引きした場合とで、管理対象機器（4100）のIPアドレスが違っている実例を示す。

図23に実際に計測した際のプログラムを示す。本プログラムはUNIXのシェルスクリプトである。行末の矢印（-->）は表示の都合上折り返されているだけで、本当は1行であることを示している。

図24ないし図26に計測結果を示す。各試行は、1行目が試行番号、2行目が試行した時間を示し、3行目がインターネットワーキングにおいて標準的なDNSの実装であるISC版BINDのdigコマンドがセンタ側DNSサーバ（1000）を参照した結果に文字列処理を施し、管理対象機器（4100）のIPアドレスを抽出したもの（a、c、e）であり、4行目から6行目までがpingコマンドがキャッシュされたDNS（リゾルバがセンタ側DNSサーバ（1000）を向いておらず、プロバイダAのDNS（4500）を向いているため）を参照した場合の管理対象機器（4100）のIPアドレス（b、d、f）である。なお7行目から10行目は前記pingコマンドの付帯する出力である。

試行に用いたDNSサーバは、既にダイナミックDNSサービスを提供しているDynDNS.ORGをセンタ側DNSサーバ（1000）として用いた。試行時において、このサーバのキャッシュの生存時間の設定は1分である。なお、この1分という値はきわめて短い。

第1回目の試行と同時に管理対象機器（4100）からの更新要求を送信し、第1

回目の試行と第 2 回目の試行の間に更新が完了している。そのため、第 2 回目の試行から前記 d i g コマンドの出力（センタ側 D N S サーバ（1000）が示す管理対象機器（4100）の I P アドレス）と p i n g コマンドの出力（この試験ではプロバイダ A の D N S サーバ（4500）を参照したが、プロバイダ A の D N S サーバ（4500）はキャッシュの生存時間の影響を受ける）は、それぞれ、別の I P アドレスを示している（下線部 a = 下線部 b から下線部 c ≠ 下線部 d へと変化）。

これが収束（下線部 e = 下線部 f）するのは、第 1 6 回目の試行である。この時、第 1 6 回目の試行は第 2 回目の試行からちょうど 1 分後に試行されている。

このように、キャッシュの生存時間の影響により、どの D N S を参照するかによってアドレスのずれが生じている。しかし時間の経過とともに収束している。センタ側 D N S サーバ（1000）のキャッシュの生存時間は 1 分と短いですが、それでもこのようなずれは生じる。

このことにより、管理対象機器（4100）の I P アドレスの確認は、管理サーバ（2000）のリゾルバがセンタ側 D N S サーバ（1000）を向いている場合や、センタ側 D N S サーバ（1000）の T T L（キャッシュの生存時間）の設定が極めて短い場合などは、省略することができる。

#### 【 0 0 4 0 】

S 2 0 4 では、必要に応じて図 2 8 のようなエラーチェックをするとよい。センタ側 D N S サーバ（1000）で障害が発生している場合には、S 2 0 4 で受取る返事が不整なものになる。S 2 0 4 で受取る返事の中に管理対象機器（4100）を示すデータが含まれないなどの場合を S 4 0 2 において検出し、センタ側 D N S サーバ（1000）を切り替えてみたり（S 4 0 8 ないし S 4 1 0）、それでもだめな時は処理を中止するようにするとよい。ここで中止された場合には、管理対象機器（4100）の状態が正常であっても、管理対象機器（4100）は見失われることになる。また、センタ側 D N S サーバ（1000）の信頼性がじゅうぶんある場合には、このエラーチェックは省略することができる。

#### 【 0 0 4 1 】

S 2 0 6 では S 2 0 4 で求められた管理対象機器（4100）の I P アドレスに対して、あらかじめ合意された方式での通信をおこなっている。なお、アドレス確

認が省略できるときには、あえてIPアドレスに変換する必要はない（この場合でも、DNSを正引きした際に得られるIPアドレスで問合せをおこなう）。S208では、S206の返事が返ってきた場合には返ってきた返事を一時的に記憶し、S206の返事が返ってこなかった場合には、S206の終了コードを一時的に記憶するなどして、S216のエラー処理へ進む。

図37に、SNMPのGetRequest命令で管理対象機器（4100）のホスト名を引いた場合の出力例を示す。

図38は、S206の通信に失敗した場合として、キャッシュの生存時間の影響などでホスト名が間違っていた場合すなわち相手先ホストがSNMPを受付けるよう設定されていなかった場合、あるいは相手先ホストが存在しなかった場合の例を示す。

図39は、S206の通信に失敗した場合として、相手先はSNMPを受付けたがコミュニティ名が間違っていた場合の例を示す。

S208では、前記図38および図39の場合などのように、管理対象機器（4100）が管理サーバ（2000）からのSNMPのGetRequest命令を受付けなかった場合のエラー処理をしている。図38や図39などのSNMPのGetRequest命令でエラーとなった場合には、S206の返事はエラーはエラー出力のみに返され、標準出力には何も帰ってこないために、サンプルプログラムでは終了コードをフラグとして代入している。

図40に、SNMPのオブジェクトIDの指定間違いの場合を示す。この場合は該当するオブジェクトIDの値が正常に返され、SNMPのGetRequest命令におけるエラーにはならないために、S212で判定されるべきである。サンプルではsysLocationを用いている。

その外、S206の通信が正常であってかつ合意された返事と違う返事が返された場合には、S212で判断される。

S210では、この通信の返事に対して、文字列処理をして、管理対象機器のホスト名（FQDN）を抽出する。

#### 【0042】

S212では、この返事を管理サーバ（2000）に設定された、管理対象機器（

4100) からの返事であるべき、あらかじめ合意された方式での通信に対する答えられるべき返事との比較をおこない、判定する。

#### 【0043】

あらかじめ合意された方式での通信に対する、管理サーバ (2000) に登録された管理対象機器 (4100) から答えられるべき返事と、管理サーバ (2000) からの問合せ (合意された方式での通信) に対して実際に管理対象機器 (4100) が答えてきた返事とが一致した場合 S 2 1 4 では、管理対象機器 (4100) は正常に動作し真性なホストである。

#### 【0044】

ここで S 2 1 4 および後述する S 2 1 6 の結果表示の出力手段であるが、キーボードとディスプレイ装置からなる通常のコンソールあるいは端末装置に出力してもよいし、記憶装置に保存されるログファイルとして書出するか、あるいは S y s l o g や X、S N M P T R A P などの T C P / I P 上の通信路を経由して別のホストに出力してもよい。また、S M T P サーバプログラムへの入力としてつなぐことによってメール送信でき、後述する保守に連係させる際に都合がよい場合もある。これらは複数を組合わせて出力してもよいし、もちろん紙媒体へ印刷出力してもよい。サンプルプログラムでは、単に標準出力に対して書出しているが、本発明を実施する場合には前記の出力方法からその環境に最適な方法で出力するか、あるいは後続する処理に進むようにするとよい。

#### 【0045】

出力結果 (サンプルプログラムのメッセージ例) を図 3 1 に示す。

管理対象機器 (4100) が真性なホストであることが確認された場合には、後続する処理に接続することができる。例えば M R T G や O p e n V i e w などによる通常 (管理対象機器が固定 I P アドレスであり、真性チェックを必要としない場合と同等) の監視処理をあげておく。通常の監視 (= 後続する処理) の例として、ucd-snmp-4.2.1 および mrtg-2.9.17 を用いてみた。M R T G は、現在のネットワークのトラフィックの状態および時間によって変化する情報 (例えば、C P U 負荷率など) をグラフィカルに表示してくれるソフトウェアツールである。M R T G は S N M P マネージャの機能を含んでいる (そのため、ここでは S N M P

マネージャとして扱った) が、トラフィック履歴ファイル生成用に特化している (つまりユーザー・インターフェースを持たない) ために、通常は別途 SNMP マネージャと組合わせて用いる。通常の管理方法については、本発明の対象外なので説明しないが、接続の際に問題があったので、その解決方法については以下に説明する。ここで試験の結果、MRTGではIPアドレスが変化するホストに対しては、管理対象機器をFQDNで指定しても (IPアドレスの変化に追従できず)、通常の監視をおこなうことはできなかった。そのため、MRTGで指定する管理対象機器名にその時点での管理対象機器 (4100) のIPアドレスを代入したMRTGの設定ファイルを生成しなおす処理を追加することによって、通常の監視処理に接続した。

#### 【0046】

ここで念のためにネットワーク管理の必要性について説明する。まず、用語の説明として、ネットワーク管理自体は、いわゆる構成管理や課金管理などをも含む通常の管理の概念であって、その対象をネットワークとしているものである。つぎに、管理と監視の関係は、ネットワーク管理という大カテゴリの中で、ホストや網そのもの (例えば、トラフィック (= 流量) は個別のノードに対してだけでなく、全体に対しても計測できる) の監視という具体的な手法があるものと解されたい。ネットワークの状態は常に変動しているために、その状態を監視することが障害対応の第一であり、また、ネットワーク設計へのフィードバックや将来の拡張計画の根拠資料となるべきものである。

しかし本発明では、管理対象機器 (4100) は動的IPアドレス割当てを受けたカスタマネットワークの境界ノードあるいは境界ノードと一体となって参照されるホストであり、きわめて小規模なものである。しかし、何らかのTCP/IP サービスを提供するのであるから、回線断やシステム障害などによって、サービス提供ができなくなっているにもかかわらず気づかずにいたのでは、問題がある。そこで、なんらかの障害が発生した場合に、すみやかに通知され復旧すべきと考えて、このような小規模なネットワークにおいてもネットワーク管理は必要なものであるとして、従来管理することのできなかったIPアドレスが変化するホストにおいても管理できるようにしようというものである。

## 【0047】

一致しない場合 S 2 1 6 は、管理対象機器 (4100) はインターネットに接続されていないか何らかの問題でセンタ側 D N S サーバ (1000) に対する更新が出来ない状態にある。

図 3 2 が出力結果 (サンプルプログラムのメッセージ例) で、(A) が返事がなかった場合、(B) が返事はあったが、一致しなかった場合である。この場合でもサンプルスクリプトでは、標準出力に対して書出しているだけだが、ログファイルなどに書出すようにした方がよい。管理対象機器 (4100) がセンタ側 D N S サーバ (1000) に更新要求したタイミングと偶然重なったために管理対象機器 (4100) で障害が発生しているように見えてしまう場合などは 2 回目の監視タイミングまで待てば、自然と正常状態に収束するはずである。このような場合には、障害として検出しない方がよい場合がある。図 2 9 にあるように、管理サーバ (2000) では、監視プログラムをタイマー実行しているため、エラーフラグをたてることにより、1 回目の異常 (S 6 0 6) と 2 回目の異常 (S 6 0 8) とを別々に検出することができる。(この場合において、図 3 0 下線部のように (フローチャートでは図 2 9 を図 2 7 の部分としたために表現できなかったが、図 2 7 S 2 1 4 の下で) 正常復帰時にエラーフラグを消去した方がよい)

## 【0048】

図 3 3 が 2 回目の出力結果 (サンプルプログラムのメッセージ例) で、(A) が返事がなかった場合、(B) が返事はあったが、一致しなかった場合である。タイマー実行による 2 回目の S 2 1 6 (S 6 0 8) では、管理対象機器 (4100) が見失われていることが明らかなので、単にログファイルに書出だけではなく、アラートをあげるなりポケベルを鳴らすなりメールにて通知するなどの方法で、何らかの後続するアクションへとつなぐようにするとよい。この場合の後続するアクションとは、復旧段階のことである。図 1 7 のように、例えば、管理対象機器 (4100) あるいは管理対象機器 (4100) に接続された L A N 上にシリアルコンソールを用意しておき、電話回線などが考えられるが第二の保守経路を経由して管理対象機器 (4100) の復旧をはかるなどをするといよい。

## 【0049】

SNMPは通信可能な状態であれば、管理対象機器(4100)のシステムの状態をほぼ何でも知りうる。また、設定変更も可能である。

本発明ではSNMPの強力な管理機能を利用することが目的ではなく、見失われがちな動的IPアドレス割当てを受けた本来なら特定できないホストが、本当に意図している相手として正しいかどうかを確認しようとするものである。ここで、後続する従来の管理に接続しようとするならば、後続する管理の方法はSNMPである可能性が高い。この場合、SNMPは管理対象機器(4100)においてすでに利用可能な状態となっているはずのもののなので、この環境をそのまま利用するものとして、SNMPを真偽の判定に用いてみた(後続する管理が不要な場合やSNMP以外の方法で真性確認をおこなう場合については後述する)。

SNMPを合意された通信の方式に用いる上で、セキュリティ上、以下の点に注意した方がよい。本発明では実験環境としてコミュニティ名は初期値であるPUBLICを用いたが、初期値のままでは侵入者を含め誰でもアクセスできてしまうため、本番環境ではPUBLICやPRIVATEなどの初期値を決して用いてはいけない。また、管理サーバ(2000)のIPアドレスがわかっている場合には、管理サーバ(2000)のIPアドレス以外からのアクセスを受付けないなどのアクセス制御もあわせておこなうべきである。

#### 【0050】

##### 実施例 2

実施例1と同様の環境であって、かつ同様にSNMPをあらかじめ合意された通信の方式に用いるものであって、sysNameの替わりに、sysNameと比較して使うことの出来る文字列の制限が少ないsysLocationを用いる事もできる。この場合にあっては、プログラム中で管理対象機器(4100)を指す変数とあらかじめ合意された方式での通信の返事をかねることが妥当でないため、あらかじめ合意された方式での通信の返事のための変数を別途用意することによって、実施例1と同様のプログラムで管理対象機器(4100)の真偽を判定できる。

#### 【0051】

すなわち実施例1において、合意された返事は省略可能だが、たとえ合意され

た返事が明示されなくとも F Q D N が暗示されることによって、合意された返事はなくてもよい訳ではなく F Q D N を省略時の値とすることによって、存在していることになる。ここで、F Q D N はセンタ側 D N S サーバ (1000) に登録されるホスト名である。

なお、設定に必要な項目は図 4 7 を参照されたい。

#### 【0052】

実施例 1 では、管理対象機器名を F Q D N として、合意された返事そのものであったため、管理対象機器 (4100) が複数あっても、合意された返事が重複することはなかった。

これは F Q D N はあらかじめ一意性が保証されているため、他の管理対象機器 (4100) と混同されることがないからである。

つぎに、なぜ明確な合意なく真性が確認できるのかについて説明する。図 4 6 のように、管理サーバ (2000) は管理対象機器 (4100) に対して I P アドレスで問合せをする。ダイヤルアップのホストであってかつダイナミック D N S を利用することが前提であるので、管理対象機器 (4100) の逆引きホスト名は、プロバイダ (あるいは I P アドレスの割当てを受けた各利用組織) のドメインに対するホスト名を返すか、あるいは逆引き設定されていない場合は、単に I P アドレスを返す。よって管理対象機器以外のホストが I P アドレスから、センタ側 D N S サーバ (1000) に設定される F Q D N を導き出すことができない。管理対象機器 (4100) が、センタ側 D N S サーバ (1000) に設定される F Q D N を返事として応答するのであれば、真性の管理対象機器 (4100) 以外に知り得ないことを知っていることになるので、管理対象機器 (4100) は真性であることが確認できる。なお、センタ側 D N S サーバ (1000) への更新をのっとるような攻撃については別論であり、これはダイナミック D N S を運営するセンタ側 D N S サーバ (1000) で対処すべき問題である。

#### 【0053】

また、F Q D N を用いることには、もうひとつの意味がある。実施例 1 や実施例 2 の方法では、管理対象機器 (4100) の真性確認は、安全でない通信路をデータの暗号化もしないままやりとりすることになる。そこで、パケット盗聴に対抗



し得る方法として、もともと盗聴されてもかまわない情報のみ通過させることにした。ここで、センタ側DNSサーバ(1000)に設定されるFQDNは、外部から管理対象機器(4100)(あるいは管理対象機器と一体となってなんらかのサービスを提供するホスト)にアクセスするために用いられる公開された情報である。したがって、当然に盗聴されたとしてもなんら問題のない情報である(ただし、SNMPコミュニティ名を盗聴されると実はよろしくない。この回避方法はアクセス制御することであり、SNMPを用いない方法を実施例5以降で説明する)。

#### 【0054】

pingとは、ICMPプロトコルのエコー要求を実装したプログラムとして、従来はホストの到達性(活死)確認に用いられてきた。ところがこのpingはIPアドレスが変化するホストに対しては利用することができない。本発明では、IPアドレスが変化するホストに対してはpingが利用できなくなったことを代替することにも利用できるようにしたいので、処理的にもプロトコル的にも軽量であることが望ましく、暗号化しなくても済むということは、軽量であることに貢献する。

#### 【0055】

実施例2において、管理対象機器(4100)が複数ある場合で、合意された返事が重複する場合に、管理対象機器(4100)を管理サーバ側で間違えると、別の管理対象機器が正常稼動しているから、管理対象機器(4100)が正常に稼動しているという誤った管理をしてしまうおそれがある。したがって、実施例2(および実施例5ないし実施例8)のFQDNでないものを合意された返事として用いる場合には、管理対象機器(4100)の数だけ、合意された返事の組を用意した方がよい。しかし、管理サーバ(2000)が管理対象機器(4100)を間違えることがないなら、返事は仮にすべての管理対象機器(4100)で共通でもかまわない。

#### 【0056】

##### 実施例3

実施例1および2は管理対象機器(4100)が直接ダイヤルアップしていた。実施例3では、管理対象機器(4100)が直接ダイヤルアップするのではなく、間に

ネットワーク接続機器が介されており、このネットワーク接続機器がダイヤルアップする場合である。

I S D N ルータなどと呼ばれるダイヤルアップルータ、あるいはブロードバンドルータなどと呼ばれる P P P o E、P P P o A、D H C P などによって I P アドレスを取得でき I P マスカレードなどの動的なネットワークアドレス変換（以下、「N A T」とする）を用いて複数の L A N 上のパソコンにグローバルサービスを受けさせるようなネットワーク接続機器（以下、「N A T B O X」とする）がダイヤルアップし、管理対象機器（4100）はカスタマの L A N にのみ接している場合（図 50 の接続形態 4 ないし接続形態 6 のいずれかを参照）には、ネットワーク接続機器に静的 N A T あるいはポートフォワーディングなどの設定をすることによって、管理対象機器（4100）が直接ダイヤルアップしていなくても（直接インターネットに接していなくても）実施例 1 や実施例 2 と同様に管理サーバ（2000）から真偽の判定ができる。

この場合の条件はダイヤルアップする機能が管理対象機器（4100）でなくネットワーク接続機器であること、静的 N A T あるいはポートフォワーディングなどの設定がネットワーク接続機器になされていることなどをのぞけば、管理対象機器（4100）に S N M P エージェントを実装されておりかつ設定されていることを含め、実施例 1 および 2 と同様である。

#### 【0057】

##### 実施例 4

実施例 3 と同様に計算機が直接にダイヤルアップするのではなくネットワーク接続機器がダイヤルアップする場合において、ダイヤルアップルータなどのネットワーク接続機器が S N M P を実装していれば、これを管理対象機器（4100）として利用することが出来る。

U N I X の場合は、I P アドレスを割当て可能な装置はすべてホストと呼ばれる。本発明では、この考え方を援用してルータや N A T B O X であろうとも、I P アドレスが割当てられていれば、ホストと呼ぶこととする。すなわち、実施例 4 ではダイヤルアップするルータが管理対象機器（4100）たるホストである。管理対象機器（4100）は S N M P を実装していることからダイヤルアップルータな

どのネットワーク接続機器である（図 5 0 の接続形態 2 参照）が、この際に、前記ルータに I P マスカレードなどの動的 N A T の機能があれば、前記ルータに D N S への動的更新する機能がない場合でも、L A N 上のパソコンに D N S 更新させることもできる（図 5 0 の接続形態 3 を参照）。

この場合においては、ダイヤルアップルータにセンタ側 D N S サーバ（1000）に登録され動的更新されるホスト名と同じ名前を設定すれば実施例 1 と同様に管理サーバ（2000）から管理対象機器（4100）の真偽を判定することができる。しかし、実施例 2 のように `s y s L o c a t i o n` を用いてより柔軟な任意の文字列を、管理対象機器（4100）が返すべき返事として合意した方がスマートな構成となる。

#### 【 0 0 5 8 】

##### 実施例 5

実施例 5 は、あらかじめ合意された通信の方式に、D O M A I N （D N S）を用いるものである。

管理対象機器（4100）は計算機であり、B I N D を実装しており、バージョン情報が設定されているものとする。ここでは、あらかじめ合意された通信の方式に D O M A I N （D N S）を用い、双方で合意された返事にこのバージョン情報を用いるものとする。

管理対象機器（4100）は、直接ダイヤルアップ接続しているか、あるいはネットワーク接続機器経由で静的 N A T あるいはポートフォワーディングの設定がされているものとする。

管理サーバ（2000）では、監視プログラムをタイマー実行している。

その他の条件や設定内容は実施例 1 と同様とする。

準備段階として、以下の件が合意され設定されているものとする。

管理サーバ（2000）には、管理対象機器（4100）名とあらかじめ合意された方式での通信に対する返事の組あるいはペアテーブルが作成され登録されているものとする。

管理対象機器（4100）に設定される、あらかじめ合意された方式での通信に対する答えるべき返事は管理対象機器（4100）で動作する B I N D が返す任意の文

字列に変更されたバージョン情報とする。

#### 【0059】

グローバルなインターネット向けの名前サービスを提供していない場合でも、局域的なLAN環境のために管理対象機器(4100)はDNSサービスを提供することができる。

図41に、管理対象機器(4100)において設定する、BINDにおけるバージョン情報の設定の仕方を示す。

BINDの標準的な動作として、このバージョン情報は明示的に設定されていないと、図44のように通常はプログラムそのもののバージョンを返す。もともとはネットワークを経由した攻撃者に対して、プログラムのバージョン情報がわかると攻撃する時の方法も明らかになるので、攻撃者の手間を増やすために、バージョン情報をわざと変更していたものである。しかし任意に設定できることから、これをあらかじめ合意された方式での通信に対する返事として用いることができる。

#### 【0060】

ふたたび図27を参照されたい。

S202およびS204はアドレス確認である。実施例1と同様である。

S206では上で求められた管理対象機器(4100)のIPアドレスに対して、あらかじめ合意された方式での通信をおこなっている。

S208では、返事が返ってきた場合には返ってきた返事を一時的に記憶し、返事が返ってこなかった場合には、S206の終了コードを一時的に記憶する。

図42に、digでBINDにおけるバージョン情報を引いた場合の出力例を示す。下線部が管理サーバ(2000)に設定された、管理対象機器(4100)からの返事であるべき、あらかじめ合意された方式での通信に対する答えられるべき返事にあたる部分である。

ここには任意の文字列を用いることができるが、実施例2と同様に管理サーバ(2000)では、返事の重複による複数の管理対象機器(4100)間での混同を避けるために、どのような返事を合意するかに気をつける必要がある。

図43に、管理対象機器(4100)がかつて割当てられていたIPアドレスを現

在割当てられているホストが存在しない場合および、管理対象機器 (4100) がかつて割当てられていた IP アドレスを割当てられている誤認されたホストが存在する場合であって、その誤認されたホストで BIND が動作していなかった場合を示す。

エラー出力に出力されるエラーのみ四角で囲んであり、その他は標準出力に出力されるエラーである。

図 44 に、管理対象機器 (4100) がかつて割当てられていた IP アドレスを割当てられている誤認されたホストが存在する場合であって、その誤認されたホストで BIND が動作していた場合を示す。この場合は dig コマンドの出力としてはエラーにならないために、S212 で判定されるべきである。

S210 では、この通信の返事に対して、文字列処理をして、管理対象機器で動作する BIND のバージョン情報を抽出する。

S212 では、この返事を管理サーバ (2000) に設定された、管理対象機器 (4100) からの返事であるべき、あらかじめ合意された方式での通信に対する答えられるべき返事との比較をおこない、判定する。

あらかじめ合意された方式での通信に対する管理対象機器 (4100) が返す答えられるべき返事と管理サーバ (2000) に登録された答えられるべき返事とが一致した場合 S214 では、管理対象機器 (4100) は正常に動作し真性なホストである。S214 では、実施例 1 と同様にログファイルなどに書出すなり後続する通常の監視へ進むなりした方がよい。

一致しない場合 S216 でも、実施例 1 と同じようにすればよい。

#### 【0061】

##### 実施例 6

実施例 6 は、あらかじめ合意された通信の方式に、SMTP を用いるものである。

管理対象機器 (4100) は計算機であり、SMTP サーバを実装しているものとする。ここでは、あらかじめ合意された通信の方式に SMTP を用い、双方で合意された返事に管理対象機器 (4100) のホスト名 (FQDN) を用いるものとする。

管理対象機器（4100）は、直接ダイヤルアップ接続しているか、あるいはネットワーク接続機器経由で静的NATあるいはポートフォワーディングの設定がされているものとする。

管理サーバ（2000）では、監視プログラムをタイマー実行している。

その他の条件や設定内容は実施例 1 と同様とする。

準備段階として、以下の件が合意され設定されているものとする。

管理サーバ（2000）には、管理対象機器（4100）名とあらかじめ合意された方式での通信に対する返事の組あるいはペアテーブルが作成され登録されているものとする。

管理対象機器（4100）に設定される、あらかじめ合意された方式での通信に対する答えるべき返事は管理対象機器（4100）に設定されたホスト名そのものとする。

#### 【 0 0 6 2 】

SMTPサーバに接続した時には多くの場合、図 4 5 のようなメッセージを出力する（例はSMTPサーバとしてもっとも普及しているSENDMAILの場合であるが、SENDMAILに次いで普及しているQMAILの場合でも、メッセージ中にホスト名が含まれるか含めることができる）。

このメッセージには、ホスト名がFQDNで表示（図 4 5 下線部参照）されているので、これを管理対象機器（4100）が真性であるかどうかを判定する識別子すなわち合意された返事に用いることができる。

#### 【 0 0 6 3 】

##### 実施例 7

実施例 7 は、あらかじめ合意された通信の方式に、HTTPを用いるものである。

管理対象機器（4100）は計算機であり、ウェブサーバを実装しているものとする。ここでは、あらかじめ合意された通信の方式にHTTPを用いる。すなわち、管理対象機器（4100）で待受けするサービスがウェブサーバであることから、双方で合意された返事には、どのような文字列でも用いることができる。

管理対象機器（4100）は、直接ダイヤルアップ接続しているか、あるいはネッ

トワーク接続機器経由で静的N A Tあるいはポートフォワーディングの設定がされているものとする。

管理サーバ (2000) では、監視プログラムをタイマー実行している。

その他の条件や設定内容は実施例 1 および 2 と同様とする。

準備段階として、以下の件が合意され設定されているものとする。

管理サーバ (2000) には、管理対象機器 (4100) 名とあらかじめ合意された方式での通信に対する返事の組あるいはペアテーブルが作成され登録されているものとする。

管理対象機器 (4100) に設定される、あらかじめ合意された方式での通信に対する答えるべき返事は管理対象機器 (4100) で動作する H T T P サーバが返す文字列中に埋め込まれた任意の文字列とする。

#### 【 0 0 6 4 】

計算機系の技術者以外の人にとっても馴染み深いものであるために、おそらくウェブサーバは、管理対象機器 (4100) もしくはカスタマのネットワークにおける T C P / I P サービスを提供するサーバにおいて、もっとも提供したいサービスのひとつだろう。H T T P では、どのような文字列でも転送することができることから、これを合意された通信の返事として利用可能である。多くのウェブサーバはファイル名の指定がない場合は、多くの場合 i n d e x . h t m l という名前のファイルが開かれる (ウェブサーバからクライアントへ転送されるの意味である) が、ここに返事となるべき文字列を記述しておくだけでよい。例えばトップページの i n d e x . h t m l 中、本文の 3 ワード目の文字列を合意しておくなどである。しかし、これでは更新の際に誤って本文の 3 ワード目の文字列を変更してしまったりすることがあるので、別のファイル名を合意しかつそのファイル中の特定の文字列を返事として合意しておいた方がよい。また、H T M L 文の < M E T A > 文中に埋め込むこともできるし、< T I T L E > を合意した返事として用いることもできる。要するに、H T T P を用いる場合には、合意された通信の方式と意図された返事の境界があいまいになる。例えば U R L 中に特定のディレクトリ名とファイル名を含む場合、これは通信の方式と考えるべきであろう。では、ここで転送された H T M L 文中の本文の 3 ワード目は、返事とみなす

べきだろうか？ これもやはり通信の方式として合意すべきだが、実施例 1 や実施例 2、あるいは実施例 5 のようなプロトコルによる制約がない分、より具体的な合意が必要であることに注意した方がよい。

また、HTTPS を合意された通信に用いる場合であって、管理対象機器 (4100) に SSL サーバ証明書が組み込まれている場合には、シリアルナンバやフィンガープリントか、あるいは単にオーガニゼーション名やカンパニー名、サーバ名などのいずれかを利用することもできる。

実施例 1 や実施例 2 の場合は、管理対象機器 (4100) の確認をする管理サーバ (2000) 以外からのアクセスを制限する方向であったが、実施例 1 や実施例 2 と違い、通信の方式に HTTP を用いる場合は、むしろ公開サーバとして、より多くの人から確認できるようにしたい場合に有効であろう。

ところで、HTTP は通常 TCP ポートの 80 番で待受けするが、しばしば別のポート番号に意図的に変更して待受けされることがある。このような場合でも、変更された TCP ポート番号が管理サーバ (2000) と管理対象機器 (4100) の間で合意されていれば、管理対象機器 (4100) が真性のホストであるか否かを確認するために用いることができる。

また、静的 NAT でもポートフォワーディングでもないが実施例 3 との複合型として、NAT BOX は、例えば 88 番ポートで NAT BOX 自体の設定変更のためのウェブアクセスを受付け、80 番ポートでリバースプロキシが動作しているような場合には、リバースプロキシによる転送先ウェブサーバにおいて、実施例 7 のあらかじめ合意された通信を実装可能である。

## 【0065】

### 実施例 8

実施例 8 では、管理対象機器 (4100) がダイヤルアップルータあるいは NAT BOX 経由で接続している場合と管理対象機器 (4100) が直接ダイヤルアップをしている場合とを問わず、管理対象機器 (4100) の記憶装置に任意の情報を答えるべき返事として保存し、あらかじめ合意された任意の方式での通信に対して前記保存された情報を記憶装置より読み出し、少なくとも前記情報を含めた返事を返信することさえ出来れば、通信の方式を問わずに管理対象機器 (4100) が真性



のホストであるか否かを確認するために用いることができる。この例は実施例7の通常でないTCPポートで待受けするウェブサーバの例をすでに挙げた。あるいはFTPサーバへクライアントが接続する際に表示されるウェルカムメッセージもあらかじめ合意された通信の方式として用いることができる。その外、管理サーバ(2000)と管理対象機器(4100)の間で合意されていれば、独自プロトコルなどの一般的でない(ウェルノウンでない)通信の方式でも同様に合意された通信の方式として用いることができる。

#### 【0066】

管理対象機器(4100)は、機能的に以下に分割され得る。aのダイヤルアップするホスト、bのダイナミックDNSへ動的更新をするホスト、cの管理対象機器(4100)である。これらの機能は、各機能毎のホストに分散されていてもよいし、各機能が1のホストに集約されていてもよい。これらの関係は、ネットワークの接続形態によって影響される。

管理対象機器(4100)のカスタマネットワークにおける接続形態を図50にまとめる。

モデム上部の雷型の線は電気通信回線を意味し、その上部にある楕円はネットワーククラウドを意味する。最上部の小さく描かれた四角が管理サーバ(2000)である。

モデムとは、通常変復調装置を指すが、ここではケーブルモデムやADSLモデム(やTA)などを(あるいはデジタル回線終端装置(=Digital Service Unit)や光終端装置(=Optical Network Unit)などがあるときは、説明の便宜上これをも)含み、ルーティング機能を提供しない、通信路上の物理的な境界を構成する装置を指すこととする。図50ではモデムを独立した装置として描いたが、ネットワーク接続機器や計算機に組み込まれている場合がある。モデムに類する機能が、ネットワーク接続機器や計算機に組み込まれている場合には、ネットワーク接続機器や計算機としてあつかうこととする。よって本発明では、モデムは通信の機能上必要なものであっても、TCP/IP的なネットワーク境界を構成しないことから、モデム単独については考慮しないものとする。

図50で、モデムのすぐ下に描かれているものは、必ずダイヤルアップする機能を有するものである。これに属するものは、ネットワーク接続機器と計算機がある。

ネットワーク接続機器とは、ルーティング機能あるいはプロトコル変換機能を提供し、TCP/IP的なネットワーク境界を構成する装置を指すこととする。図50では、「ルータなど」と表記している。

計算機とは、利用者によってプログラム可能なものを計算機と呼ぶこととし、仮に計算機がネットワーク接続機器と同様の機能を有している場合であったとしても、この点においてネットワーク接続機器と区別されることとする。利用者端末などもこれに含まれる。

#### 【0067】

以下各接続形態に応じて、管理対象機器(4100)がどの装置であるかを中心に説明する。

実施例1の典型を接続形態1とする。これは、計算機が直接ダイヤルアップする場合である。実施例2も同じである。この形態では、bのDNS更新するホスト、cの管理対象たるホストがaのダイヤルアップするホストと同一の場合である。この場合において、aのダイヤルアップするホストすなわち計算機がネットワーク境界を構成する。このことから、例えばNATを実装している場合やVPNトンネリングしている場合のようにネットワーク接続機器の機能を有しているか、アプリケーションゲートウェイを構成していれば、破線部分の計算機に対して、ネットワーク接続を提供することも可能である。

実施例4は、ネットワーク接続機器を介して計算機が接続される場合であって、ネットワーク接続機器がcの管理対象機器(4100)である場合である。典型例が接続形態2である。また、接続形態2に対して、ネットワーク接続機器がDNS更新できない場合に、bのDNS更新するホストを計算機とした場合が、接続形態3である。

実施例3および実施例5ないし実施例8では、aのダイヤルアップするホスト、bのDNS更新するホスト、cの管理対象たるホストなどが機能的に分割され、この機能が計算機およびネットワーク接続機器に分散されている場合である。

この場合の典型が接続形態6である。ここで、例えば接続形態4の場合は、ネットワーク接続機器がセンタ側DNSサーバ(1000)に対してダイナミックDNS更新できる場合であって、かつ管理対象機器(4100)たりえない場合にこのような構成をとることができる。なお、接続形態4ないし接続形態6において、aのダイヤルアップするホストはルータなどとされているが、接続形態1の応用としてこれは計算機によっても代替し得る。ここで、ネットワーク接続機器がダイヤルアップすることを明示している実施例3および実施例4を除けば、一般に計算機はネットワーク接続機器と比してソフトウェアを追加することによってcの管理対象機器(4100)としてもbのDNS更新するホストとしても用いることができることから、接続形態1はどの実施例にも用いることができる。すなわち実施例3および実施例4(ネットワーク接続機器がダイヤルアップすることが明記されている場合)を除き、aの位置にあるルータなどは計算機であってもよい。この場合、aのダイヤルアップするホストには、少なくともcの管理対象機器(4100)に対して静的NATあるいはポートフォワーディングなどが設定されているものとする。図50ではモデムのすぐ下にaのダイヤルアップするホストがあるが、この下には計算機だけではなく、ネットワーク接続機器があってもよい。これはカスタマネットワークを構成するLANが多段のLANを構成していてもよいことを示す。

実施例5ないし実施例8は、すべての接続形態で用いることができる。ただし、実施例5ないし実施例8を接続形態2や接続形態3に適用する場合には、ネットワーク接続機器がサインに対し、カウンターサインを返しうるように構成できる必要がある。

#### 【0068】

aのダイヤルアップするホスト、bのダイナミックDNSへ動的更新をするホスト、cの管理対象機器(4100)は、同一のLAN上(あるいは同一の場所)に設置されるものとするすると、広域のネットワークから見れば、このLANは網端側にあることになる。ここで広域のネットワークをインターネットとした場合(正確にはNATを必要とする場合)、広域のネットワークを経由した通信では、a、b、cのそれぞれを識別することはできない。よって、このLANは外部

に対して単一のネットワークノードのように振舞う、計算機およびネットワーク接続機器の集合である（インターネット・サービス・プロバイダーへの端末型ダイヤルアップのようにLANを構成しておらず、端末一台のみの場合にあって同じである）。これを本発明では、カスタマネットワークもしくはエンドサイトと呼ぶこととする。エンドサイトは特に広域のネットワークから見た場合のエッジ側を指すものとして扱うが、着目点が違うだけで同じ物を指している。図50のモデム以下の点線で囲まれた部分である。接続形態1から接続形態6は、カスタマネットワークの内訳であり、管理サーバ（2000）から見れば、カスタマネットワークが接続形態1から接続形態6のいずれの類型に属しようとして、a、b、cのそれぞれを識別することはできないという点で共通している。そのため、管理サーバ（2000）ではカスタマネットワークの構成や管理対象機器（4100）がカスタマネットワークのLAN上でどこに、位置しているかについて考慮する必要がない。

#### 【0069】

なお、カスタマネットワークはプライベートIPアドレスが使用されている状態を仮定している。このため、インターネットからは、カスタマネットワークに対して、直接ルーティングされることはない。aのダイヤルアップするホストは、インターネットとカスタマネットワークの接点を構成する。ルーティングはaのダイヤルアップするホストで止まるから、インターネットからb、cには直接到達できない。

上記は、広域のネットワークをインターネットとした場合であった。

ところが、広域のネットワークとしては、インターネット以外にも、第一種電気通信事業者や第二種電気通信事業者が提供するあるいは自営網によるインターネットに接続されない、TCP/IPによるネットワークが考えられる。この場合には、NATを前提とするのではなく、ルーティングによって別のネットワークにあるセンタ側DNSサーバ（1000）や管理サーバ（2000）から管理対象機器（4100）へのアクセスが、直接に管理対象機器（4100）に到達できる場合がある。

。

#### 【0070】

実施例 1 ないし実施例 8 では、説明上インターネットと表現してきた。しかし、グローバルなインターネットでのみ本発明は実施可能なものではなく、実際は TCP/IP を用いた通信でありさえすればよい。

カスタマネットワークと外部ネットワークの関係を図 49 に示す。

①は、インターネット・サービス・プロバイダーへの端末型ダイヤルアップのように LAN を構成しておらず、端末一台のみの場合を指す。NTT のフレッツ・ADSL（登録商標）などがこれに該当する。この場合は LAN を構成していないが、インターネットに接しているために、やはりネットワークに接続されている（スタンドアロンではない）ものとみなす。LAN を構成していないことから、カスタマネットワークは存在しないのではとの議論がありうるが、ループバックのみのカスタマネットワークが存在し、WAN 接続されているものと考えればよい。③および⑤は、①に準ずるものとする。

②は、代表的なインターネット接続の場合である。これまでの説明は、このパターンを想定して、説明してきた。以下、このパターンとの相違点がどのように影響するかについて、説明する。

④は、第一種電気通信事業者や第二種電気通信事業者が提供するインターネットに接続されない、TCP/IP によるネットワークを WAN とする場合である。パソコン通信やフレッツ（登録商標）オフィスなどがこれに該当する。②の場合と同様に扱って問題ない。DNS サーバが私設のものであることは、従来からあるプライベートネットワークに使用するドメイン名の命名規則において制限があるのみで、本発明には影響しない。

⑥は、自営網による場合である。自営網は一般に組織内の利用のために、専用線（および類似の役務。例として ATM メガリンクや IP-VPN などを挙げておく）などによって構成され、ルーティングされているものをいう。④の場合は、IP-VPN などの契約がなければ通常はカスタマネットワーク（の内側。網端までは当然に到達するので）へのルーティングは提供されない。しかし、第一種電気通信事業者や第二種電気通信事業者が提供する役務であって、ルーティングがされる場合は、⑥に含めて考えた方が筋道がよい。ネットワーク境界を越えて、外部ネットワークがルーティングによって直接にカスタマネットワーク上の

ホストにアクセスできる場合である。すなわち、この場合は、管理対象機器 (4100) がモデムのすぐ下に位置しない場合であっても、a のダイヤルアップするホストは上流の網から IP アドレスを動的に割当てられるのではなく、カスタマネットワーク上の DHCP サーバ (DHCP リレーされている場合を含む) から IP アドレスを動的に割当てられ、かつ管理対象機器 (4100) であるという点で、図 50 の接続形態 1 ないし接続形態 3 に相当することになる。ところで、古くから自営網を運用している会社や大学の中には、IP アドレス体系がグローバル・アドレスになっているところがある。このような自営網は、インターネットそのものの構成要素であるものと考えてさしつかえない。

⑧は、LAN のみで構成されたネットワークにあって、LAN が多段となっている場合である。例を挙げると、1 の事業所であって、フロア毎に別の部に分かれている場合に、各フロアが事業所内バックボーン・ネットワークを経由して相互に接続されている場合などである。WAN が存在しておらず、インターネットに接続しない場合やインターネットに接続しない広域のネットワークに接続しない場合か、仮にインターネットに接続していたとしてもこの接続を無視できる (セキュリティポリシーが強力な組織などにあってインターネットなどへ接続する際に障壁が大きい) 場合であるという特徴を除けば、自営網の場合と酷似する。ここで、LAN が多段になっているとは、単にハブなどによって多段となっているだけではなく、論理セグメントが分かれており、ルーティングされている状態を指す。この場合、管理サーバ (2000) の接する LAN が管理対象機器 (4100) の接する LAN とは別の LAN であれば、管理対象機器 (4100) の接する LAN をカスタマネットワークと考え、④⑥と同じと考えればよい。

以上は、物理セグメントと論理セグメントがともに分かれている場合であったが、例外として、物理セグメントが 1 で論理セグメントのみ 2 以上に分かれている場合、例えば 1 のインターフェースに異なるネットワークに属する 2 以上の IP アドレスを割当て、これを中継するよう構成されたゲートウェイ装置などがある場合には、単一の (=一段の) LAN の場合と同様となる。

⑦は、単一の LAN の場合である。本発明は実施可能だが、LAN が一段のみの場合すなわち外部ネットワークがまったく存在しない場合には、TCP/IP

的な中継を要せず、各ホストがすべて直接かつローカルに通信できるので、動的 IP アドレス割当てのホストであっても、わざわざ私設の DNS サーバを参照することなく、TCP/IP 以外のプロトコルによって、真性確認をした方が現実的であろう。

当然のことであるが、管理対象機器 (4100) がスタンドアロンの場合を、本発明では考慮していない。通信する相手が存在しないからである。

なお、②④⑥の場合は⑧と共存する。

以上によって、(⑦の場合に意味があるかどうかは別論だが) ①ないし⑧のすべてのパターンで本発明を実施可能である。

### 【0071】

ここで図 48 に、主に多段の LAN の場合に問題になり得る点について説明する。図 48 は、カスタマネットワークにおける LAN の内訳でもあるが、自営網の場合およびインターネットに接続されない電気通信事業者が提供する役務の場合も同様であるものとし、この場合にあってはカスタマネットワークは管理対象機器 (4100) が直接接続されている部分を指すものと考えられる。ネットワーク 1 およびネットワーク 2 は、それぞれ LAN の場合と WAN の場合がある。

図 48 には、パターン 1 ないしパターン 3 までを挙げた。パターン 2 およびパターン 3 は、図 49 における④⑥と類似のパターンであって問題がない。ここで問題となり得る場合は、パターン 1 の場合であって、ネットワーク 1 が LAN の場合である。図 49 における⑦に挙げた単一の LAN の場合と同様に、管理対象機器 (4100) と管理サーバ (2000) とが同一の LAN 上にあるため、TCP/IP 以外のプロトコルによって、真性確認をした方が現実的と考えることができる。しかし、この場合であっても、別のネットワーク上に管理対象機器 (4100) が存在し、かつここでいう管理サーバ (2000) が前記管理対象機器 (4100) をも管理するものとすれば、本発明を実施する意義はじゅうぶんにあると考える。なぜならば、別のネットワーク上の管理対象機器 (4100) を管理する際には、本発明の実施が必要なものであって、管理サーバ (2000) が集中管理するためには、管理の方法を統一した方がよいからである。なお、図 49 の⑧においてパターン 3 のように装置が配置されている場合は、図 49 の②④⑥の場合に相当し、本発明

で典型的に扱っている接続形態に相当する。

なお、TCP/IP 以外のプロトコルはルーティングされないものとする。

#### 【0072】

ここまで、場合分けして説明してきたが、複雑でわかりにくいものである。これはネットワークの接続のされ方を網羅的に説明する困難さに起因すると思われるので、以下のように、LAN か WAN かを問わず、ルーティングがどこで止まるかによって、大別できる。

ルーティングによって、直接管理対象機器 (4100) に到達できる場合には管理サーバ (2000) は、当然に管理対象機器 (4100) の 1 つ 1 つを別のホストとして識別できる。この場合においては、管理対象機器 (4100) は、ダイヤルアップする (動的アドレス割当てを受ける) 機能と、ダイナミック DNS 更新する機能と管理対象機器 (4100) であることの機能を備えていなければならない。そして、この場合は、比較的単純な場合である。

ルーティングがダイヤルアップするホストで止まる場合には、ダイヤルアップするホストにおいてポートフォワーディングなどによって、外部ネットワークからは管理対象機器 (4100) に管理サーバ (2000) からのアクセスが到達するようにするかダイヤルアップするホストを管理対象機器 (4100) としなければならない。これはルーティングによって到達できる場合と比べてやや複雑であり、具体例についてはすでに実施例として詳述した。ダイヤルアップする (動的アドレス割当てを受ける) 機能と、ダイナミック DNS 更新する機能と管理対象機器 (4100) であることの機能は、独立した 3 のホストが担ってもまた 1 のホストが担ってもよいが、外部からはカスタマネットワークの代表として、管理対象機器 (4100) が確認されるという点で特徴がある。

#### 【0073】

##### 実施例 9

ルータなどで、設定変更用のウェブインターフェースを有する場合は、ウェルノウンポート (RFC 1700 ASSIGNED NUMBERS でいうところのウェルノウンポートと同じか類似するもの) に従って 80 番ポートで待受けする。ファイヤウォールなどの一部の機器は、例えば 88 番ポート (などの 80 番ポート以外のポ



ート)で設定変更のためのウェブアクセスを待受けする場合がある。最近のエンドサイト向けのこれらの製品はWAN側とLAN側に分かれてインターフェースを用意しており、多くの場合、WAN側ポートにはアクセス制御が施されている。

ここで、ネットワーク接続機器において(ファイヤウォールでなくとも)、設定変更のためのウェブアクセスの待受けを88番ポート(などの80番ポート以外のポート)でし、アクセス制御されるものとする。この際、80番ポートで通常のウェブアクセスを待受け、これにはアクセス制御などを施さないものとする。80番ポートでリバースプロキシを動作させ、リバースプロキシによる転送先ウェブサーバにおいて、実施例8のあらかじめ合意された通信を実装可能とするのも手なのだが、ここで、装置にはホスト名が登録されるものとし(エンドサイト向け製品の内、低価格製品の多くはこのような装置にはホスト名の設定ができないものがある)、このホスト名はダイナミックDNSによって動的更新されるセンタ側DNSサーバ(1000)にて設定されるFQDNで登録されるものとし不揮発メモリなどの記憶装置に保存され、80番ポートへの通信要求を受けた際に、前記保存されたFQDNを記憶装置より読み出し、該FQDNすなわちホスト名を含めた文字列を返信するように構成する。

#### 【0074】

管理サーバ(2000)が管理対象機器(4100)に対して通信を試みる方法として、このように実施例4のようにネットワーク接続機器に対して、実施例7のようにHTTPを合意された通信の方式として用い、実施例1のように(SNMPのsysNameではなくHTTPだが)FQDNを返事として合意した方法などのように実施例を組合わせた方法として用いることができる。なお、カスタマネットワーク上の位置だが、図50の接続形態のすべての場所だけでなく、接続形態6における計算機の位置にあっても、すでに説明したように機能するものであって、ここで構成した装置がネットワーク接続機器であった場合に、配下に別のネットワークを有している場合が考えられる。また、ここで構成した装置が直接図50におけるaのダイヤルアップするホストである必要は必ずしもない。

#### 【0075】

このとき仮に、ここで述べた機器が図50にいうaのダイヤルアップするホストであって、ネットワークの到達性からNATを必要とするネットワークである場合には、80番ポートを上記のようなサイン・アンド・カウンターサインに用いてしまうと、ウェブサービスを提供する際にポートフォワーディングなどが必要であるから、ウェルノウンでないポートをアナウンスしなければならなくなる。これでは、カスタマネットワークにおいてウェブサービスを提供しようとする場合の利便性をそこなうことになるから、ウェブサービスを提供したい場合には、類似のポートでサインを待受けするようにするとよい。すなわち、HTTPアクセスを待受けするポートにおいて、機器設定用のポート、サイン・アンド・カウンターサインを用いたネットワーク管理用のポート、一般の閲覧に供するためのウェブサービスを提供するウェルノウンなポート（ただし、ここで述べた機器が応答するのではなく、ポートフォワーディングなどしてもよい）のように3種類のポートで待受けするように構成することもできる。

これを実施例9とする。実施例9では通信の方式をHTTP固定とし、返事をFQDNとすることによって、単純化した。通常、ネットワーク接続機器にあっては、いわゆる計算機に比して拡張性に劣るものである。これは、例えば機能追加する際に単にプログラムを追加実装すればよいというものではなく、ファームウェアの書換えなどが必要であって、利用者によっては、簡単にできないなどの問題があるものである。そこで、実施例9は、ルータやNATBOXなどのように記憶装置の容量に制限があるネットワーク接続機器に対しても、あらかじめコンパクトに実装しておくことが可能である。

#### 【0076】

管理対象機器（4100）としては、ネットワーク接続機器だけでなく、もちろん計算機であってもよいし、コンパクトに実装可能なことから、専用のシステムでもよい。この場合、専用のシステムは、単に管理サーバ（2000）に真性確認させるためだけの機能を有しておればよく、インターフェースももちろん1でよい。例えば、図50の接続形態6の場合であって、cに位置していたとすると（図50では計算機だが、これが上記専用のシステムの場合）、ダイヤルアップするホストの外側にあるネットワークがインターネットなどのルーティングによって管

理対象機器 (4100) に到達できないネットワークである場合に、ダイヤルアップするホストに静的 NAT やポートフォワーディングなどが設定されていれば、外部ネットワークからはシステムに到達可能である。この場合において、システムは単に LAN 上の IP アドレスを割当てられていれば、外部ネットワークからは、一体となって参照されるために、ここでいう専用のシステムが真性確認できれば、管理サーバ (2000) からは、カスタマネットワークおよびその境界ノードが真性であることが確認される。つまり、ここでは、単に実施例 9 を実装した 1 のインターフェースを有する機器を準備すれば、ポートフォワーディングなどの設定をダイヤルアップするホストにするだけで、真性確認できることになる。このような装置は、単純なために、安価に製造することができるし、完成品ではなく組込み用の基盤あるいはキットとしても提供できる。また、これをソフトウェアとして実装すれば、計算機に用いる場合でも、設定作業を省略化することができる。この場合は、記憶装置に述べた記憶媒体読取り装置に実装される取り外し可能な記憶媒体とすればよい。

#### 【0077】

サインはあらかじめ合意された通信の方式の上位概念であって、単にカウンターサイン (合意された方式での通信に対する答えられるべき返事を返信すること) をうながす働きをする。この場合において、サインを受取った通信相手が、そのサインを理解できないようなら、その通信相手はサインの送り手が想定していた通信相手ではない。すなわち、管理対象機器 (4100) ではない。

サインの出し方もカウンターサインの内容も、相方の合意に基づくべきものである。そのため、多くのパターンが考えられることから、サインの仕方、カウンターサインの内容を多く例示してきた。

以上見てきたように、TCP/IP ネットワークにおいて IP アドレスが変化するホストを特定するためにダイナミック DNS を用いるが、なおダイナミック DNS の特性のために誤認されたホスト (4200) でなく管理対象機器だと認識されているホストとして本当に正しい通信相手 (真性なホスト) であることを明らかにすることができない場合において、

図 1 のように、サインとして通信の方式を合意し、管理サーバ (2000) から管

理対象機器 (4100) に対してサインでもって問合せをし、管理対象機器 (4100) はサインに対するカウンターサインを返信する。この時、管理サーバ (2000) では管理サーバ (2000) 内に設定される管理対象機器 (4100) 毎の (サインと) カウンターサイン (の組あるいはペアテーブルの登録情報) と照合することによって、管理対象機器 (4100) が真性であるか否かの確認をおこなうことができる。

#### 【0078】

##### 実施例 10

実施例 1 ないし実施例 9 は、管理サーバ (2000) 側から管理対象機器 (4100) に対して順にポーリングをおこなうものであった。実施例 10 では、管理対象機器 (4100) の方から自律的に行動を起こす場合を示す。

#### 【0079】

管理対象機器 (4100) から管理サーバ (2000) へのアライブメッセージを送信する。

メッセージ送信時において相手が正常に受取ったかどうかの確認もなく、したがって再送も発生しない場合を除けば、送信側から見れば単純な送信であったとしても、受信側からは送信側に対して少なくとも ACK、NAK の応答などによる双方向の通信でもって送信処理は成立っている。このような場合でも通常単に「送信」という表現がとられるため、ここでは以下に例示する認証などといったややインテリジェントな処理が含まれてはいるが、一連のセッション (通信のかたまり) として、ここでは単に「アライブメッセージの送信」としている。

管理サーバ (2000) では、管理対象機器 (4100) からのアライブメッセージを受付ける際に、認証をおこなうものとする。なお、管理サーバ (2000) では、認証をおこなうことから、仮に管理対象機器 (4100) になりすまされたアクセスを受けた際にも、管理サーバ (2000) のシステムへの侵入を阻むように設定すべきであることに注意されたい。この方法については従来の技術であり、当業者であるならば理解されることであろうから、本願では単に注意すべきこととして挙げるに止める。

#### 【0080】

認証はユーザ名でおこなう。ユーザ名と管理対象機器 (4100) 名の組は一意的な

組であるものとする、ユーザ名から、どの管理対象機器 (4100) からのアライブメッセージであるかを導き出せる。よって、管理対象機器 (4100) からのアライブメッセージを認証後受領したことによって管理サーバ (2000) において、管理対象機器 (4100) についてわかることは、以下のことである。

- ① 管理対象機器 (4100) が生存していること。
- ② 管理対象機器 (4100) が真性であること。
- ③ 管理対象機器 (4100) の I P アドレス。
- ④ アライブメッセージの到着時間。(=最終管理対象機器 (4100) 生存確認時刻)

管理サーバ (2000) では、管理対象機器 (4100) から送信されたアライブメッセージを認証に成功したときに受領し、認証に失敗したときには破棄する。ただし、失敗の際にもユーザ名および発信元 I P アドレスは記録するものとする。

#### 【 0 0 8 1 】

アライブメッセージは送信されるものとしているが、管理サーバ (2000) で認証に成功して初めて受けられるものであるから、単にパケットを投げればよいという類の通信ではなく、ハンドシェイク後認証というコネクション型の通信をする必要がある。

コネクション型の通信として、例えば T C P による通信が考えられる。認証は、従来であれば、正規利用者本人だと確認する過程 (例えば、システムにログインする権利の確認あるいはファイルシステムへのアクセス権を獲得する過程) であった。しかしここでは、利用権限の正当性を確認することではなく、管理対象機器 (4100) の識別に用いる。

#### 【 0 0 8 2 】

ここでは、従来のパスワード認証を用いる場合を説明することとする。

この場合、通信の方式としては、認証できるものであれば、どのような通信の方式でもかまわない。主にシステムのアカウントを利用する方法に、t e l n e t や f t p が挙げられる。システムのアカウントを利用しないものとして、H T T P の C G I 認証などが挙げられる。以下、f t p を利用した例を挙げることにする。ただし f t p は認証機能のみ利用し、ファイル形式変換機能やファイル転

送機能などの認証以外の機能は利用しないものとする。よってここでアライブメッセージは、管理対象機器（4100）から管理サーバ（2000）への一連の F T P コネクションである。

#### 【 0 0 8 3 】

管理対象機器（4100）と管理サーバ（2000）の双方で合意され、設定されるべき内容を図 4 7 に示す。

管理対象機器（4100）が U N I X の場合は、図 5 3 のシェルスクリプトを実行する。

ここで、ftp に対するオプション -n は、ftp が最初に接続する際の自動ログインを無効化（非対話型のインターフェースで実行）するためのオプションである。これによって、EOF までをクライアント側から制御することが可能になる。mgr.center.names4commerce.com は管理サーバ（2000）のホスト名である。hbuser01 hbpass01 はそれぞれ、ユーザ名およびパスワードである。

W i n d o w s 機の場合は、f t p クライアントの中から、ユーザ名とパスワードを指定可能なオートパイロット機能のあるプログラムを選べばよい。その他、専用のシステムであれば、U N I X の例を参考に実装する。

#### 【 0 0 8 4 】

管理サーバ（2000）では、管理対象機器（4100）からの通信に対して認証ログを記録する。これによって、過去にさかのぼって、管理対象機器（4100）が、少なくともいつまではアライブメッセージを送ってきていたか（すなわち管理対象機器（4100）がいつまで生存していたか）などを追跡することができる。

#### 【 0 0 8 5 】

管理サーバ（2000）では、以下のログが残される。

図 5 4 に、認証に成功したときの例を示す。

図 5 5 に正しくないパスワードのため、認証に失敗したときの例を示す。

このうち、

Sep 10 21:04:19 mgr ftpd[20008]: FTP LOGIN FROM tokyo-ppp36.korai.or.jp as hbuser01 (図 5 4 の下線部)

が、管理対象機器（4100）の識別に用いることができる。すなわち、ユーザ名

と送信元ホスト名が含まれ、認証に成功したことを示している行である。これを管理対象機器 (4100) からのアライブメッセージと呼ぶこととする。実施例 2 に管理対象機器 (4100) 名と返事に別々の文字列を使う場合の返事が管理サーバ (2000) 上の管理対象機器 (4100) の設定情報において重複しないようにした方がよいことを説明したが、実施例 10 では管理対象機器 (4100) 名とユーザ名は 1 対 1 に対応されなくてはならない。ユーザ名から管理対象機器 (4100) 名を一意に導くことができれば、認証は管理対象機器 (4100) の生存確認に用いることができる。ここで、表示される接続元ホスト名 `tokyo-ppp36.korai.or.jp` は、ダイナミック DNS の習性により、管理対象機器 (4100) の IP アドレスがプロバイダ (あるいは IP アドレスの割当てを受けた各利用組織) のドメインに対するホスト名に化けたもの (逆引き設定されていない場合は、最初から IP アドレスを返すので、この行の処理は不要) であるので、このホスト名を正引きすることによって、この時点での管理対象機器 (4100) の IP アドレスが求められる。

#### 【0086】

以上が、管理対象機器 (4100) から管理サーバ (2000) へ、管理対象機器 (4100) が自律的にその生存を知らせる場合の方法である。

しかし、アライブメッセージの最終到達時間が古い場合 (例えば 3 日前でも 12 時間前でも) であるときに、現在の管理対象機器 (4100) がどうなっているかを知ることができない。そこで現在と近似するほど古くない過去において管理対象機器 (4100) の生存確認がされている状態を保つ必要がある。こうすることによって、この状態が保てなくなれば、管理対象機器 (4100) に障害が発生したとすることができる。この方法を以下に示す。

#### 【0087】

管理対象機器 (4100) からのアライブメッセージの送信が定期的におこなわれれば、管理対象機器 (4100) が障害に陥ったことも検出可能である。すなわち、管理対象機器 (4100) からのアライブメッセージが途切れたことによって、管理対象機器 (4100) が障害に陥ったことがわかる。

図 5 1 のように、管理対象機器 (4100) がアライブメッセージ送信プログラム (例えば、図 5 3 のようなものである) をタイマー実行し、定期的にアライブメ

ッセージを送信する。

管理サーバ (2000) では、前記管理対象機器 (4100) 毎のレコードの中でタイマー時間も合意しておく。ただし、ここでのタイマー時間は、プログラムがタイマー実行される時間間隔を示すものであり、通信において用いるものではないため、図 47 に挙げる設定項目には含めないこととした (ただし合意されている必要はある。このような情報が、付加情報である)。このタイマー時間はプログラムをタイマー実行させる OS 上の仕掛け (UNIX なら `cron`、Windows なら `at` コマンドなどの、あるいはネットワーク接続機器なら当該機器が備えているスケジュール機能など) によって、設定されるべきものである。

しかし、この場合においては管理対象機器 (4100) は、認証可能な通信をタイマー実行できるものに限られる。計算機の場合はもちろん可能だが、ネットワーク接続機器を管理対象機器 (4100) として用いる場合には、スケジュール機能をもったものに限られる。

管理サーバ (2000) で管理対象機器 (4100) の障害発生を最遅で検出できる時間を、時間「a」とすると、

時間「a」＝タイマー時間＋遅延時間＋余裕時間

となるので、これを超えて、管理対象機器 (4100) からのアライブメッセージの到着 (認証の成功) が検出できなければ、管理対象機器 (4100) は障害に陥っている。遅延時間は、中継される網の混雑やホップ数、中継ルータの処理性能、管理サーバ (2000) や管理対象機器 (4100) の処理性能や CPU の負荷が大きいことによって発生する。

このことから、ログから最後のアライブメッセージの到着時間と現在の時刻の差を計算し、この時間差が前記時間「a」より長い場合に、管理対象機器 (4100) が障害であることを検出するプログラム (図 52) をタイマ実行すればよい。

障害が検出されたときは、実施例 1 の S216 と同様の障害通知をおこなえばよい。

#### 【0088】

上で障害が検出されたときに、何らかの理由で (例えば、管理対象機器 (4100) を再起動しているタイミングなど) 管理対象機器 (4100) は、異常でないにも



かかわらずアライブメッセージの送信ができないことがあり得るために、実施例 1 と同様に 2 度目の障害検出を待ってもよい。

2 度目の障害検出で管理対象機器 (4100) が障害に陥っていることを検出すればよい場合には、時間「a」を算出するためにあらかじめ遅延時間を計算する必要がなくなる。

このとき、管理サーバ (2000) では、

時間「a」＝管理対象機器 (4100) で定期的のアライブメッセージを送信する際のタイマー時間

時間「a」＝管理サーバ (2000) で図 5 2 のプログラムを実行するタイマー時間

とすれば、

管理サーバ (2000) で実行される図 5 2 のチェックで 2 回連続して、障害が検出されたときに、管理対象機器 (4100) は障害に陥っているといえることになる。なお、2 回目の検出は実施例 1 の図 2 9 のように、フラグを用いて検出すればよい。そのため、管理対象機器 (4100) と管理サーバ (2000) でそれぞれプログラムの実行が同期されなくても (マシン時間が同期されていなくても) タイマー時間の 2 回分を限度 (最遅) としての障害検出が可能になる。

#### 【0089】

最初の障害検出のときに 2 度目の検出を待つかわりに、実施例 1 ないし実施例 9 のいずれかの方法で、管理サーバ (2000) の方から管理対象機器 (4100) に確認プロセスをおこなうことによって、管理対象機器 (4100) が障害状態に陥っていることを確認することもできる。

また、この場合において、管理対象機器 (4100) からのアライブメッセージの到着があるかあるいはアライブメッセージの到着が途切れることを障害検出の手段とするのではなく (すなわち認証は実は重要ではなく)、実施例 1 ないし実施例 9 のいずれかの方法で管理対象機器 (4100) の活死を確認するための、単にトリガとして実施例 10 を用いることができる。

この際、実施例 10 を接続形態 6 の計算機で実施して、前記トリガによって、実施例 4 を接続形態 2 のネットワーク接続機器で行うという、1 のカスタマネッ

トワークに管理対象機器（4100）が2つあるような応用も可能である。もちろん、接続形態6で実施例10と実施例1ないし8とを2種類の管理対象機器（4100）でおこなうなどして、冗長化するのもよい。

#### 【0090】

これまで認証の方法を、「認証はユーザ名でおこなう」ものとして説明してきたが、これは既存のシステムによるログイン認証の仕組みを流用しやすかったために用いただけである。「しかしここでは、利用権限の正当性を確認することではなく、管理対象機器（4100）の識別に用いる。」と前記したとおり、「認証はユーザ名でおこなう」必要はかならずしもない。

すなわち、合意（管理サーバ（2000）にとって予期）された方法にのっとって、所定のメッセージが管理サーバ（2000）に届くことによって、管理対象機器（4100）の生存が確認できる。

#### 【0091】

サイン・アンド・カウンターサインでは、管理サーバ（2000）から管理対象機器（4100）への問合せを行い（サイン）、管理対象機器（4100）から管理サーバ（2000）への返事（カウンターサイン）が管理サーバ（2000）において予期（合意）されたものである場合に、管理対象機器（4100）が真性であるものとしていた。

ここで、管理対象機器（4100）が一方的に管理サーバ（2000）に対して、2つの独立したメッセージを順に送信したものとすると、管理サーバ（2000）では2つのメッセージの内容A、Bとその順序を照合することによって、管理対象機器（4100）が真性であるという事ができる。この方法は、認証という概念には含まれないものである。

実際には、連続して送られてくる2のメッセージにおいて、その順番と内容から管理サーバ（2000）に管理対象機器（4100）を識別させ生存確認させることができる。この際、管理サーバ（2000）では、最初に送られてくるメッセージが正しかった場合に、次のメッセージが正しいことをチェックするプログラムを書けばよい。ただし連続して送信される2のメッセージではなく、単に1のメッセージを送信する方が、タイマー時間を短くできる場合がある。

## 【0 0 9 2】

また、公開かぎ暗号方式の利用した方法を用いることもできる。例えば管理対象機器（4100）は管理対象機器（4100）を示す識別子を管理サーバ（2000）の公開かぎで暗号化し、これをアライブメッセージとして送信することによって、管理対象機器（4100）が生存しかつ真性であることを管理対象機器（4100）に知らせることもできる。この場合、管理対象機器（4100）を示す識別子は管理サーバ（2000）の公開かぎで暗号化されているため、管理サーバ（2000）の秘密かぎでしか復号することができないため、前記識別子は第三者に漏洩することはない（復号できない暗号化された情報は盗聴されてもよい）。この方法でも一応は安全性を確保できるが、悪意の第三者が適当な文字列を管理サーバ（2000）の公開かぎで暗号化して管理サーバ（2000）に送信する（公開かぎは入手可能であるので、これは可能である）と、アライブメッセージを偽造することができることとなる。管理サーバ（2000）には、前記識別子が登録されているものとする、（ここまで気にする必要があるかどうかは別として）攻撃者が識別子を推測できるなら、管理サーバ（2000）に管理対象機器（4100）の状態のいかんにかかわらず、稼動していると誤認させることができる。このような場合には、前記識別子をいったん管理対象機器（4100）の秘密かぎで暗号化した後、さらに管理サーバ（2000）の公開かぎで暗号化した後にアライブメッセージとして送信するか、メッセージダイジェストを付して生成されたアライブメッセージを送信するとよい。公開かぎ暗号方式の利用は、処理が重くなるという難点はあるが、盗聴不可、本人確認、改ざんを発見できるなどの面で優れた点が多い。

なお、管理対象機器（4100）たる装置は、実施例 9 で説明したものを用いることができる。

## 【0 0 9 3】

以上のことによって、管理サーバ（2000）側から管理対象機器（4100）に対して順にポーリングをおこなう方法だけでなく、管理対象機器（4100）の方から自律的に行動を起こす場合でも、管理サーバ（2000）と管理対象機器（4100）とが所定の通信をすることによって、管理対象機器（4100）の真性を管理サーバ（2000）に確認させることができる。

## 【0094】

## 【発明の効果】

固定的なIPアドレスを与えられたTCP/IPネットワーク上のホストの管理は、通常であれば機器監視としてpingコマンドなどを利用してホストの活死を監視することができる。しかし、ダイヤルアップのホストにあっては、そのIPアドレスが変化することから、pingによる管理では、誤った（管理対象機器でない）ホストがpingに応じていても、正常に稼動していることになってしまう。本発明では、管理対象機器（4100）が真性のホストであることを確認するようにして、これまで管理することのできなかったIPアドレスの変化するホストを、管理できるようにした。また、通常の管理をおこなう場合にも、従来であればIPアドレスが変化するホストは管理することができなかったが、通常の管理の前段の処理として本発明を用いることによって、その後のより高度な管理（例えば、CPU負荷やネットワークトラフィックの監視）をも可能とした。

## 【0095】

## 【補助的説明】

1、ログの出方を含むプログラム出力は実装やオプションに依存する。ログファイルやプログラムの在処などは、処理系によって標準的な場所が異なる。それぞれ、実施しようとする環境にあわせて実施されたい。

2、実験はインターネットのグローバルネットワーク環境をメインにおこなった。ホスト名やIPアドレスについては、実験時に利用可能なものを用いた。実験用に用意したホストもあるが、多くは実在のホストである。これらのホストはグローバルサービスを提供しているものであり、本発明と直接の関係はないものも多い。また、これらのホストが、将来に向けても実験時と同様のサービスを提供している保証はない。よって、ホスト名やIPアドレスについては、あくまでも例として見ていただきたい。本発明はやがて公開されることになるが、その際も、本発明が何らかの攻撃の一助となることを、発明者は決して望んでいない。

3、telnetコマンドやTELNETプロトコルなどのように、コマンドは小文字、プロトコルは大文字として表記した。コマンドとプロトコルの両方の

意味で通じる場合には、いずれかで表記しているが区別していない。

4、カスタマネットワーク上のサーバあるいは端末機器などの計算機はパーソナルコンピュータであることをさまたげない。

#### 【 0 0 9 6 】

##### 【公知の技術文献】

##### 【公知の技術のURL一覧】

ISC-BIND は最初のDNSの実装としてバークレー版UNIXに採用されて以来、インターネットの標準DNSである。インターネット・ソフトウェア・コンソーシアムは、BINDの開発元である。以下にURLを示す。

<http://www.isc.org/>

net-snmp はSNMPエージェントとSNMPマネージャの統合パッケージである。ucd-snmp から名前が変更されたものである。UCDはカリフォルニア大学デビス校の意味で、開発の母体であった。以下にURLを示す。

<http://www.net-snmp.org/>

MRTG (The Multi Router Traffic Grapher) は、ネットワークの負荷を監視するソフトウェアツールである。MRTGは現在のネットワークのトラフィックの状態を示すグラフィックイメージを含むHTMLページを生成する。以下にURLを示す。

<http://www.mrtg.jp/doc/> (日本語)

<http://people.ee.ethz.ch/~oetiker/webtools/mrtg/>

gnudip はダイナミックDNSをグローバルサービスとして役務提供するためのパッケージである。以下にURLを示す。

<http://gnudip2.sourceforge.net/>

DHIS はダイナミックDNSをグローバルサービスとして役務提供するためのパッケージである。以下にURLを示す。

<http://www.dhis.org/>

DynDNS はダイナミックDNSをグローバルサービスとして役務提供している業者である。以下にURLを示す。

<http://www.dyndns.org/>

names4commerce はダイナミック DNS をグローバルサービスとして役務提供している業者である。以下に URL を示す。

<http://www.names4commerce.net/>

【 0 0 9 7 】

【Domain Name System に関するRFC一覧】

- 0819 Domain naming convention for Internet user applications.
- 0881 Domain names plan and schedule. (Updated by RFC0897)
- 0897 Domain name system implementation schedule. (Updates RFC0881)
- 0920 Domain requirements.
- 0921 Domain name system implementation schedule - revised. (Updates RFC0897)
- 0952 DoD Internet host table specification.
- 0974 Mail routing and the domain system.
- 1032 Domain administrators guide.
- 1033 Domain administrators operations guide.
- 1034 Domain names - concepts and facilities. (Updated by RFC1101, RFC1183, RFC1348, RFC1876, RFC1982, RFC2065, RFC2181, RFC2308, RFC2535)
- 1035 Domain names - implementation and specification.
- 1101 DNS encoding of network names and other types. (Updates RFC1034, RFC1035)
- 1122 Requirements for Internet hosts - communication layers.
- 1123 Requirements for Internet hosts - application and support. (Updates RFC0822) (Updated by RFC2181)
- 1178 Choosing a name for your computer.
- 1183 New DNS RR Definitions. (Updates RFC1034, RFC1035)
- 1464 Using the Domain Name System To Store Arbitrary String Attributes.
- 1480 The US Domain.
- 1535 A Security Problem and Proposed Correction With Widely Deployed DNS

Software.

- 1536 Common DNS Implementation Errors and Suggested Fixes.
- 1591 Domain Name System Structure and Delegation.
- 1611 DNS Server MIB Extensions.
- 1612 DNS Resolver MIB Extensions.
- 1706 DNS NSAP Resource Records.
- 1713 Tools for DNS debugging.
- 1794 DNS Support for Load Balancing.
- 1876 A Means for Expressing Location Information in the Domain Name System. (Updates RFC1034, RFC1035)
- 1886 DNS Extensions to support IP version 6.
- 1912 Common DNS Operational and Configuration Errors.
- 1918 Address Allocation for Private Internets.
- 1956 Registration in the MIL Domain.
- 1982 Serial Number Arithmetic. (Updates RFC1034, RFC1035)
- 1995 Incremental Zone Transfer in DNS.
- 1996 A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY). (Updates RFC1035)
- 2010 Operational Criteria for Root Name Servers.
- 2052 A DNS RR for specifying the location of services (DNS SRV).
- 2065 DNS Security. (削除)
- 2104 HMAC: Keyed-Hashing for Message Authentication.
- 2136 Dynamic Updates in the Domain Name System (DNS UPDATE). (Updates RFC1035)
- 2137 Secure Domain Name System Dynamic Update. (Updates RFC1035)
- 2146 U.S. Government Internet Domain Names.
- 2163 Using the Internet DNS to Distribute MIXER Conformant Global Address Mapping (MCGAM).
- 2168 Resolution of Uniform Resource Identifiers using the Domain Name System.

stem.

2181 Clarifications to the DNS Specification. (Updates RFC1034, RFC1035, RFC1123) (Updated by RFC2535)

2182 Selection and Operation of Secondary DNS Servers.

2219 Use of DNS Aliases for Network Services.

2230 Key Exchange Delegation Record for the DNS.

2247 Using Domains in LDAP/X.500 Distinguished Names.

2308 Negative Caching of DNS Queries (DNS NCACHE). (Updates RFC1034, RFC 1035)

2317 Classless IN-ADDR.ARPA delegation. 2345 Domain Names and Company Name Retrieval.

2352 A Convention For Using Legal Names as Domain Names.

2373 IP Version 6 Addressing Architecture.

2374 An IPv6 Aggregatable Global Unicast Address Format.

2375 IPv6 Multicast Address Assignments.

2377 Naming Plan for Internet Directory-Enabled Applications.

2517 Building Directories from DNS: Experiences from WWWSeeker.

2535 Domain Name System Security Extensions. (Updates RFC2181, RFC1035, RFC1034)

2536 DSA KEYS and SIGs in the Domain Name System (DNS).

2537 RSA/MD5 KEYS and SIGs in the Domain Name System (DNS).

2538 Storing Certificates in the Domain Name System (DNS).

2539 Storage of Diffie-Hellman Keys in the Domain Name System (DNS).

2540 Detached Domain Name System (DNS) Information.

2541 DNS Security Operational Considerations.

2553 Basic Socket Interface Extensions for IPv6.

2606 Reserved Top Level DNS Names. (Also RFC2606)

2671 Extension Mechanisms for DNS (EDNS0).

2672 Non-Terminal DNS Name Redirection.



2673 Binary Labels in the Domain Name System.

2782 A DNS RR for specifying the location of services (DNS SRV).

2845 Secret Key Transaction Authentication for DNS (TSIG).

2870 Root Name Server Operational Requirements.

**【図面の簡単な説明】**

**【図 1】** サイン・アンド・カウンターサインの動作を示す図である。

**【図 2】** インターネットのドメイン名における、ドメインツリーを示す図である。

**【図 3】** 管理対象機器もしくはカスタマネットワークにおいて、ダイヤルアップを示す図である。

**【図 4】** 管理対象機器もしくはカスタマネットワークにおいて、アドレス割当てを示す図である。

**【図 5】** 管理対象機器もしくはカスタマネットワークにおいて、DNS 更新を示す図である。

**【図 6】** 管理対象機器もしくはカスタマネットワークにおいて、正常状態を示す図である。

**【図 7】** 管理対象機器もしくはカスタマネットワークにおいて、回線断発生を示す図である。

**【図 8】** 管理対象機器もしくはカスタマネットワークにおいて、再接続を示す図である。

**【図 9】** 管理対象機器もしくはカスタマネットワークにおいて、アドレス割当て（再）を示す図である。

**【図 10】** 管理対象機器もしくはカスタマネットワークにおいて、DNS 更新（再）を示す図である。

**【図 11】** 管理対象機器もしくはカスタマネットワークにおいて、ホストの移動を示す図である。

**【図 12】** 各ネットワークにおいて、参照される DNS を示す図である。

**【図 13】** 管理対象機器もしくはカスタマネットワークにおいて、誤認を示す

図である。

【図 14】 管理対象機器もしくはカスタマネットワークにおいて、正常状態（収束）を示す図である。

【図 15】 管理対象機器もしくはカスタマネットワークにおいて、回線断のまま（図 8 以降の別パターン）を示す図である。

【図 16】 管理対象機器もしくはカスタマネットワークにおいて、回線断のままの場合の誤認を示す図である。

【図 17】 管理対象機器もしくはカスタマネットワークを保守する場合において、回線断時などにおける第二の保守経路による保守を示す図である。

【図 18】 インターネットの一般利用者が管理対象ホストを正引き名前問合せする場合において、キャッシュが有効な時の DNS の探索順を示す図である。

【図 19】 インターネットの一般利用者が管理対象ホストを正引き名前問合せする場合において、キャッシュが有効でない時の DNS の探索順を示す図である。

。 【図 20】 キャッシュの生存時間を示す図である。

【図 21】 管理対象ホストの動作および外部環境の変化を示すフローチャートである。

【図 22】 管理対象ホストの障害のパターンを示す図である。

【図 23】 キャッシュの生存時間の収束 1（計測プログラム）を示す図である。

。 【図 24】 キャッシュの生存時間の収束 2（計測結果 1）を示す図である。

【図 25】 キャッシュの生存時間の収束 3（計測結果 1 の続き）を示す図である。

【図 26】 キャッシュの生存時間の収束 4（計測結果 2 の続き）を示す図である。

【図 27】 課題を解決するための手段を示すフローチャートである。

【図 28】 課題を解決するための手段 2（S 204 のオプション処理）を示すフローチャートである。

【図 29】 課題を解決するための手段 3（S 216 のオプション処理）を示す

フローチャートである。

【図 3 0】 スクリプト 1 を示す図である。

【図 3 1】 スクリプト 1 正常出力サンプル（正常な場合）を示す図である。

【図 3 2】 スクリプト 1 エラー出力サンプル（管理対象ホストが見付けられなかった場合）を示す図である。

【図 3 3】 スクリプト 1 エラー出力サンプル（管理対象ホストが 2 度目に見付けられなかった場合）を示す図である。

【図 3 4】 D I G コマンド正常出力サンプルを示す図である。

【図 3 5】 D I G コマンドエラー出力サンプル（D N S サーバが存在しない場合）を示す図である。

【図 3 6】 D I G コマンドエラー出力サンプル（管理対象ホストが存在しない場合）を示す図である。

【図 3 7】 S N M P 正常出力サンプル（管理対象機器（4100）が真性の場合）を示す図である。

【図 3 8】 S N M P エラー出力サンプル（ホストが間違いの場合）を示す図である。

【図 3 9】 S N M P エラー出力サンプル（コミュニティ名が間違いの場合）を示す図である。

【図 4 0】 S N M P エラー出力サンプル（オブジェクト I D の指定間違いの場合）を示す図である。

【図 4 1】 B I N D におけるバージョン情報の設定のためにする設定ファイルの変更箇所を示す図である。

【図 4 2】 D I G コマンド正常出力サンプルを示す図である。

【図 4 3】 D I G コマンドエラー出力サンプル（管理対象ホストが存在しなかった場合）を示す図である。

【図 4 4】 D I G コマンドエラー出力サンプル（別のネームサーバを参照してしまった場合）を示す図である。なお、バージョン情報が設定されていない場合の標準的な出力例（正常）でもある。

【図 4 5】 S M T P サーバ（S E N D M A I L）に接続した際の最初のメッセ

ージ例を示す図である。

【図 4 6】 管理サーバ (2000) から管理対象機器 (4100) へ行きが I P アドレス、帰りが F Q D N であることを示す図である。

【図 4 7】 管理サーバ (2000) と管理対象機器 (4100) の通信に必要な設定されるべき項目を一覧で示す図である。

【図 4 8】 各ホストとネットワークの位置関係を示す図である。

【図 4 9】 カスタマネットワークと W A N の関係を示す図である。

【図 5 0】 管理対象機器 (4100) のカスタマネットワークにおける接続形態を示す図である。

【図 5 1】 管理対象機器 (4100) から管理サーバ (2000) へアライブメッセージが定期的に送信される様子を示す図である。

【図 5 2】 管理対象機器 (4100) からアライブメッセージが定期的に送信される場合に管理サーバ (2000) で実行すべき処理を示すフローチャートである。

【図 5 3】 管理対象機器 (4100) で実行される f t p によるアライブメッセージ送信プログラム (シェルスクリプト例) を示す図である。

【図 5 4】 管理サーバ (2000) での f t p 認証に成功したときのログ出力サンプルを示す図である。

【図 5 5】 管理サーバ (2000) での f t p 認証に失敗したときのログ出力サンプルを示す図である。

#### 【符号の説明】

記号	名称
1000	センタ側 D N S サーバ。ダイナミック D N S サービスを提供するサーバ。
2000	センタ側管理サーバ。
4000	プロバイダ A。管理対象機器の接続先たるプロバイダである。あるいはカスタマネットワークから見て上流のネットワーク (D.N.S サーバなどがある側) を構成し、これに接続されるネットワーク境界ノードに動的 I P アドレス割当てする機能を有するものを指す。

4100 管理対象機器。管理サーバからの管理を受けるホストである。ホストとは、TCP/IPネットワーク上のIPアドレスを割当てられた装置をいうのであって、必ずしも計算機である必要はなく、ネットワーク接続機器であってもよい。

4200 プロバイダAの別のユーザ。プロバイダAの管理対象機器以外のユーザである。別のホストあるいは誤認されたホストともいう。管理対象機器がかつて割当を受けていたIPアドレスを割当てられる可能性があるという点で、管理対象機器と誤認されるおそれのあるホストのこと。

4500 プロバイダAのDNSサーバ。

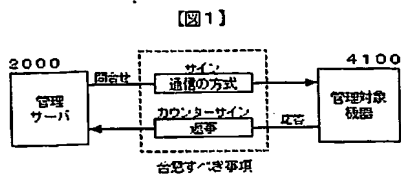
5000 プロバイダB。管理対象機器の接続先以外のプロバイダ。すなわちインターネットの一般利用者の接続先たるプロバイダである。この概念はプロバイダAがインターネットに接続しているかもしくはプロバイダAがその他のTCP/IPネットワークと相互接続されている場合にのみ有効な考え方である。

5300 一般利用者。インターネットの一般利用者。（センタ側と総称されるサーバの）管理者および管理対象機器の運用者、管理対象機器の（閲覧者を除く）直接（ローカルな）利用者から見た、第三者のことである。管理対象機器（あるいはカスタマネットワークとプロバイダAのネットワーク境界）に動的IPアドレス割当てするプロバイダAがインターネットに接続しておりかつプロバイダBがインターネットに接続しているか、もしくはプロバイダAとプロバイダBが相互接続されている場合にのみ一般利用者の概念は（管理対象機器から見て）プロバイダBの上で成立する。すなわち、プロバイダBは（プロバイダAから見て）ルーティングによって到達する別のネットワークでありさえすればよい。

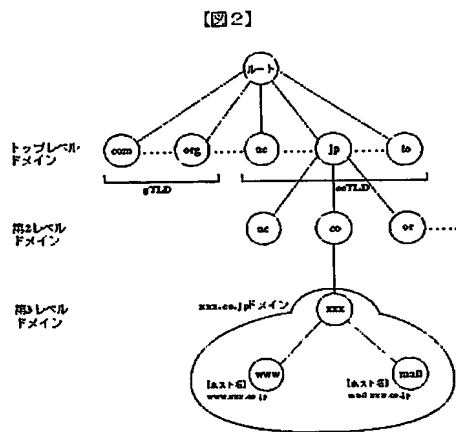
5500 プロバイダBのDNSサーバ

【書類名】 図面

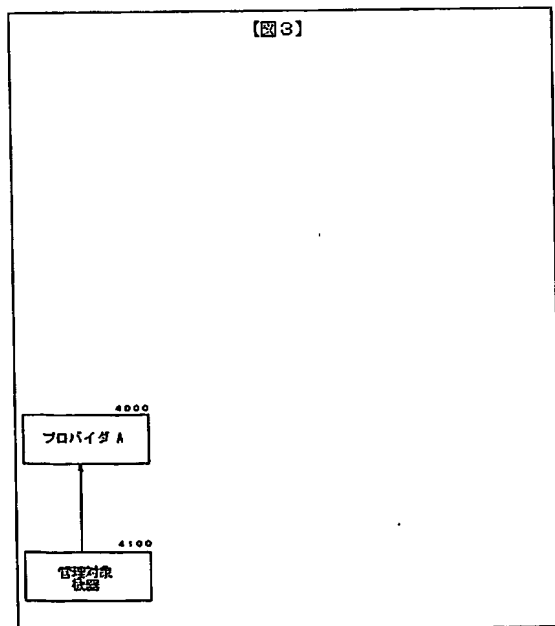
【図 1】



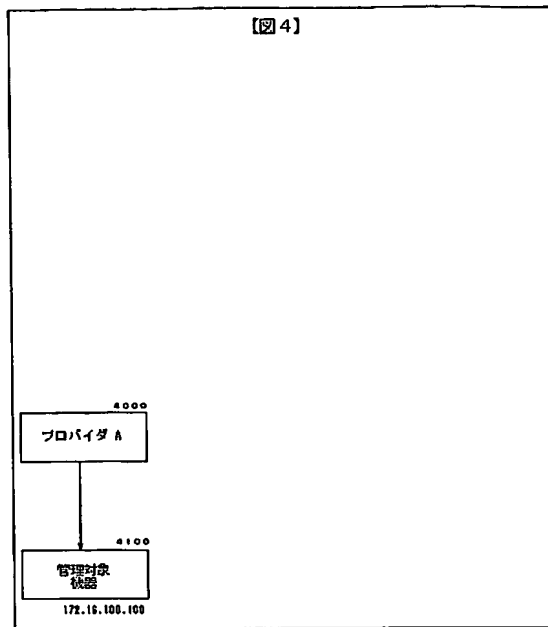
【図 2】



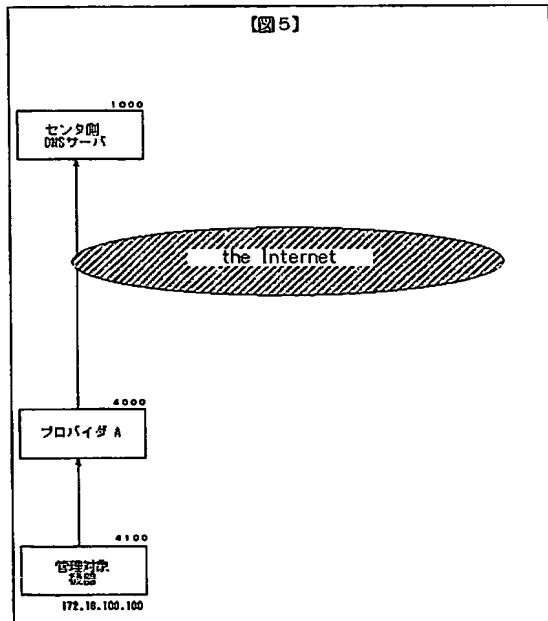
【図 3】



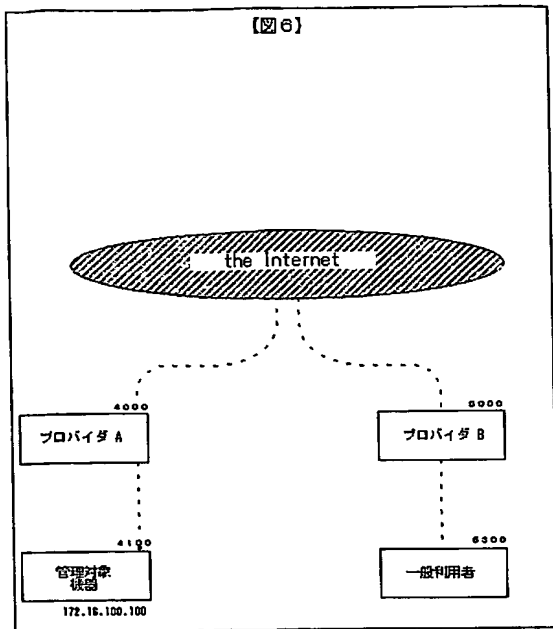
【図 4】



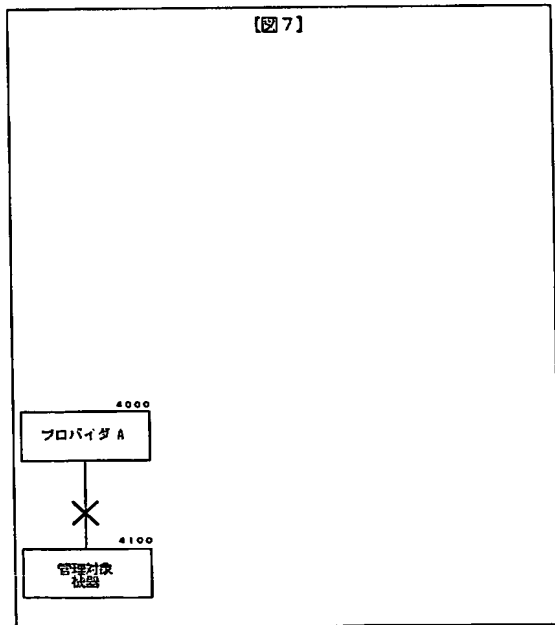
【図 5】



【図 6】

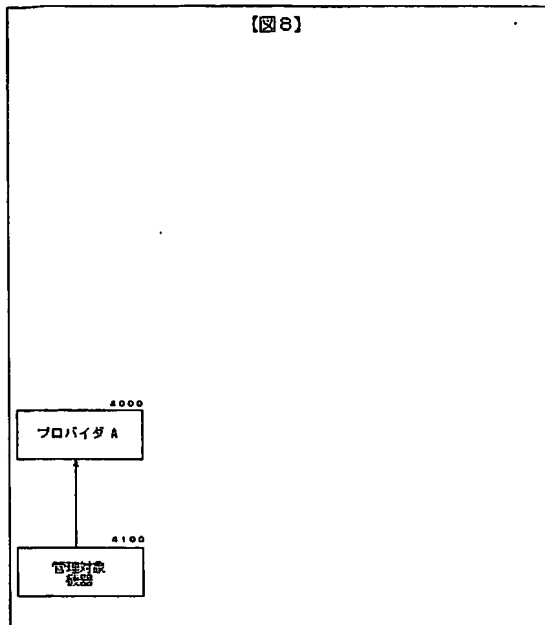


【図 7】

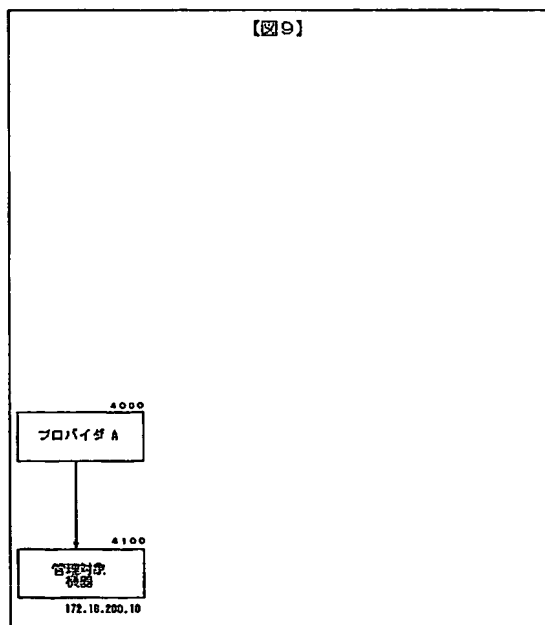




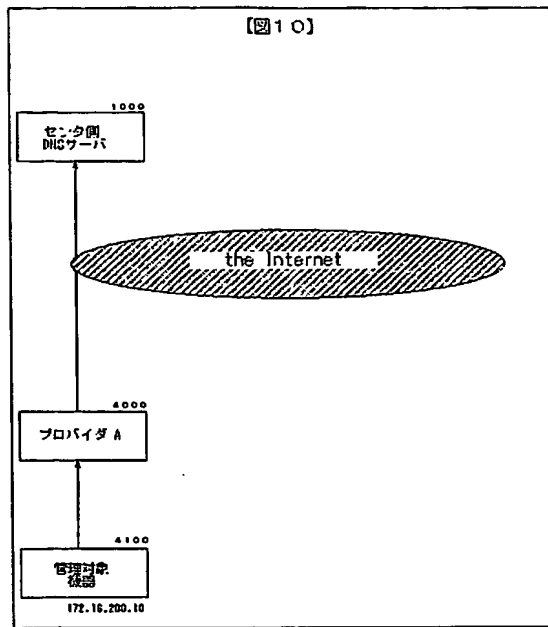
【図 8】



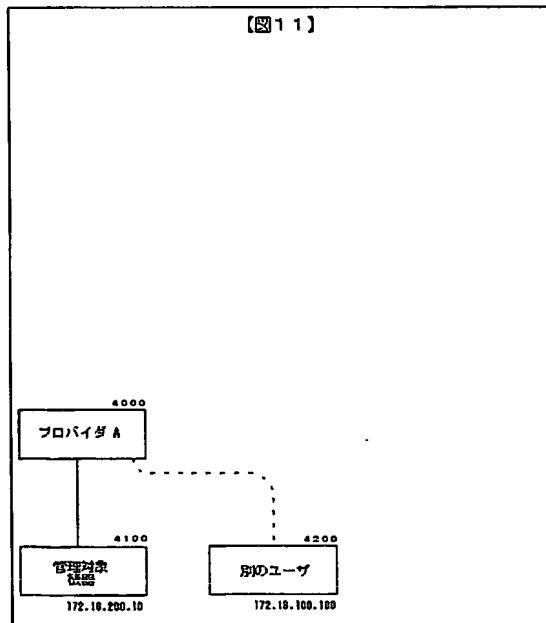
【図 9】



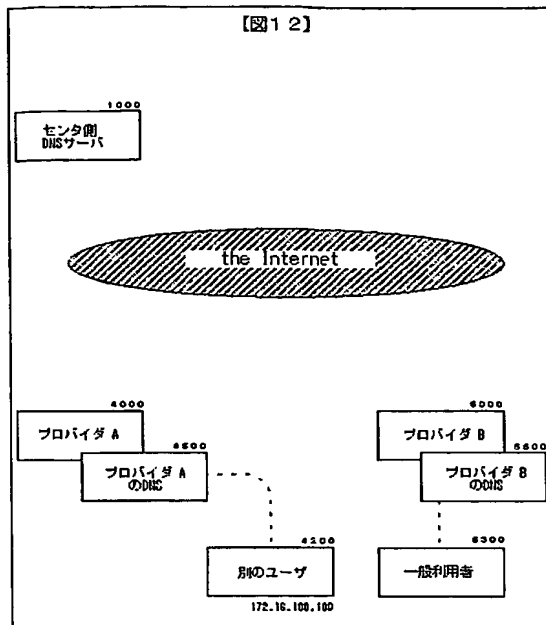
【図 10】



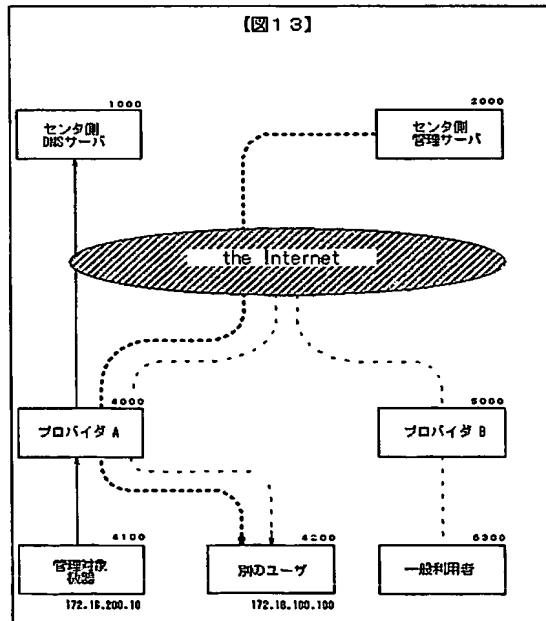
【図 11】



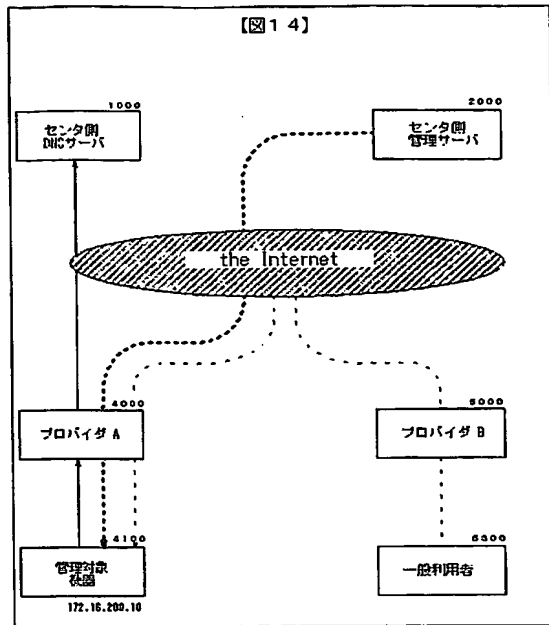
【図 12】



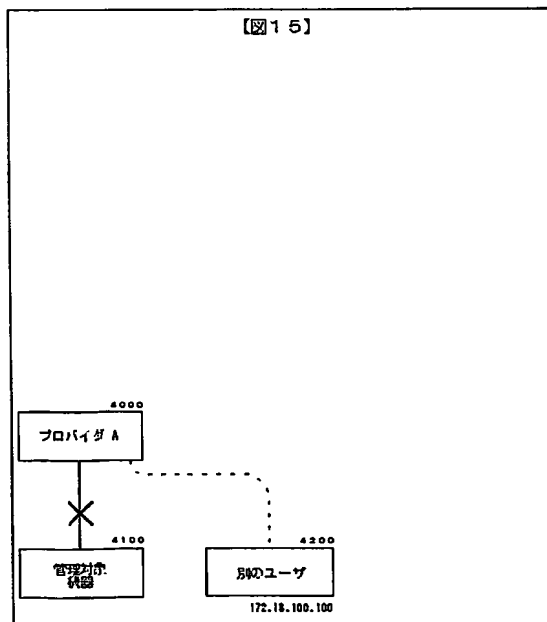
【図 13】



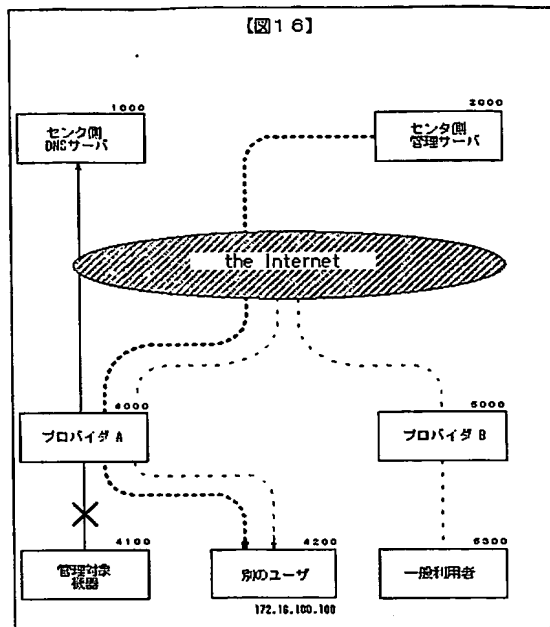
【図 14】



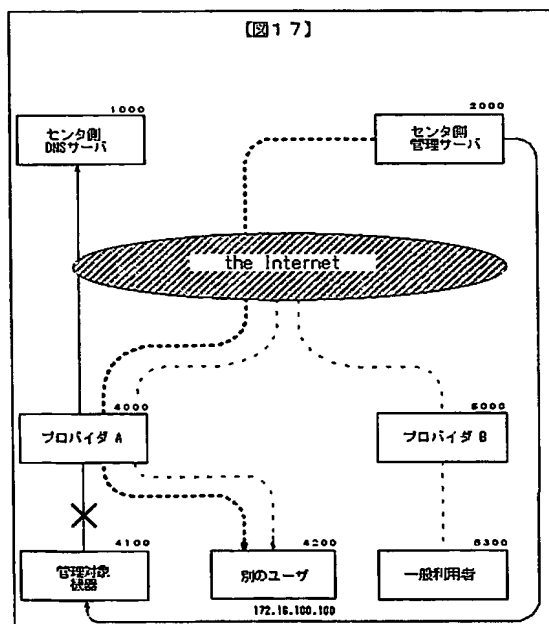
【図 15】



【図 16】

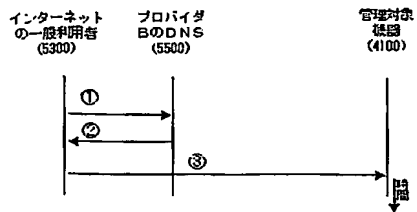


【図 17】



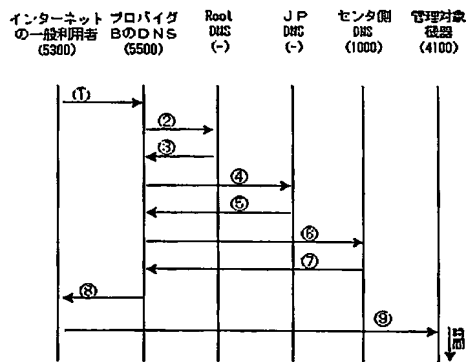
【図 18】

【図 18】



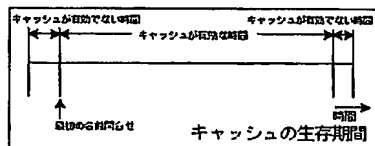
【図 19】

【図 19】

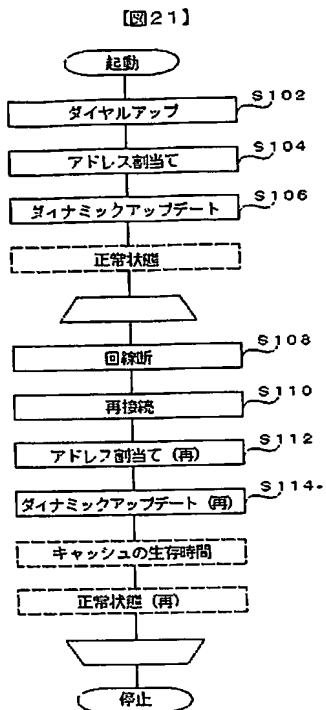


【図 20】

【図 20】



【図 21】



【図 22】

【 図22 】

管理対象 ホスト (4100)の 状態	IPアドレスの 状態	回線断時のIPアドレス= 再接続後のIP アドレス	回線断前のIPアド レス=再接続後のI Pアドレス
	回線断以前に管理 対象ホストに割当 てられていたIPアド レスを使っているホ ストが存在しない	回線断以前に管理 対象ホストに割当 てられていたIPアド レスを別のユーザ が使っている場合	回線断以前に管理 対象ホストに割当 てられていたIPアド レスが再度割当て られた
回線断のまま	アクセス不可	誤認	—
回線断後 再接続	キャッシュの 生存時間内 キャッシュされて いない場合	アクセス不可 (Q14参照)	誤認 (Q14参照)
	OK	OK	OK
DNSへのダイナミックアップ デートの失敗	アクセス不可	誤認	OK

【図 23】

【図23】

```

# 計測用スクリプト
date >> $LOG
echo -n "result of Dig i" >> $LOG
dig @209.09.32.137 bsdguru.dyndns.org | grep bsdguru.dyndns.org | -->
grep "18 A" | cut -f4 >> $LOG
ping -c 2 bsdguru.dyndns.org >> $LOG
sleep 1
  
```

## 【図 24】

【図 24】

```

# 計測結果
# sh ttlcheck.sh
#
Thu Sep 12 23:59:36 JST 2002
result of DIG :210.159.30.63 a
PING bsdguru.dyndns.org (210.159.30.63): 56 data bytes
64 bytes from 210.159.30.63: icmp_seq=0 ttl=248 time=70.998 ms
64 bytes from 210.159.30.63: icmp_seq=1 ttl=248 time=83.131 ms
b
--- bsdguru.dyndns.org ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 70.996/77.064/83.131/6.067 ms

2
Thu Sep 12 23:59:39 JST 2002
result of DIG :218.218.1.188 c
PING bsdguru.dyndns.org (210.159.30.63): 56 data bytes
64 bytes from 210.159.30.63: icmp_seq=0 ttl=248 time=84.041 ms
64 bytes from 210.159.30.63: icmp_seq=1 ttl=248 time=98.320 ms
d
--- bsdguru.dyndns.org ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 84.041/91.180/98.320/7.139 ms

3
Thu Sep 12 23:59:41 JST 2002
result of DIG :218.218.1.188
PING bsdguru.dyndns.org (210.159.30.63): 56 data bytes
64 bytes from 210.159.30.63: icmp_seq=0 ttl=248 time=81.680 ms
64 bytes from 210.159.30.63: icmp_seq=1 ttl=248 time=87.170 ms
--- bsdguru.dyndns.org ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 87.170/89.415/91.680/2.245 ms

```

## 【図 25】

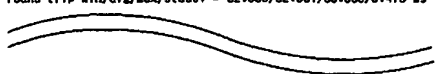
【図 25】

```

4
Thu Sep 12 23:59:43 JST 2002
result of DIG :218.218.1.188
PING bsdguru.dyndns.org (210.159.30.63): 56 data bytes
64 bytes from 210.159.30.63: icmp_seq=0 ttl=248 time=87.482 ms
64 bytes from 210.159.30.63: icmp_seq=1 ttl=248 time=70.174 ms
--- bsdguru.dyndns.org ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 70.174/78.833/87.482/6.659 ms

5
Thu Sep 12 23:59:46 JST 2002
result of DIG :218.218.1.188
PING bsdguru.dyndns.org (210.159.30.63): 56 data bytes
64 bytes from 210.159.30.63: icmp_seq=0 ttl=248 time=83.038 ms
64 bytes from 210.159.30.63: icmp_seq=1 ttl=248 time=82.086 ms
--- bsdguru.dyndns.org ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 82.088/82.561/83.038/0.475 ms

```



```

13
Fri Sep 13 00:00:32 JST 2002
result of DIG :218.218.1.188
PING bsdguru.dyndns.org (210.159.30.63): 56 data bytes
64 bytes from 210.159.30.63: icmp_seq=0 ttl=248 time=93.051 ms
64 bytes from 210.159.30.63: icmp_seq=1 ttl=248 time=97.035 ms
--- bsdguru.dyndns.org ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 93.051/95.043/97.035/1.882 ms

```



【図 26】

【図 26】

```

14
Fri Sep 13 00:00:35 JST 2002
result of DIG :218.218.1.188
PING bsdguru.dyndns.org (210.159.30.63): 56 data bytes
64 bytes from 210.159.30.63: icmp_seq=0 ttl=248 time=88.092 ms
64 bytes from 210.159.30.63: icmp_seq=1 ttl=248 time=83.185 ms

--- bsdguru.dyndns.org ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 88.092/75.638/83.185/7.547 ms


15
Fri Sep 13 00:00:37 JST 2002
result of DIG :218.218.1.188
PING bsdguru.dyndns.org (210.159.30.63): 56 data bytes
64 bytes from 210.159.30.63: icmp_seq=0 ttl=248 time=88.655 ms
64 bytes from 210.159.30.63: icmp_seq=1 ttl=248 time=81.907 ms

--- bsdguru.dyndns.org ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 81.907/90.281/98.655/8.374 ms

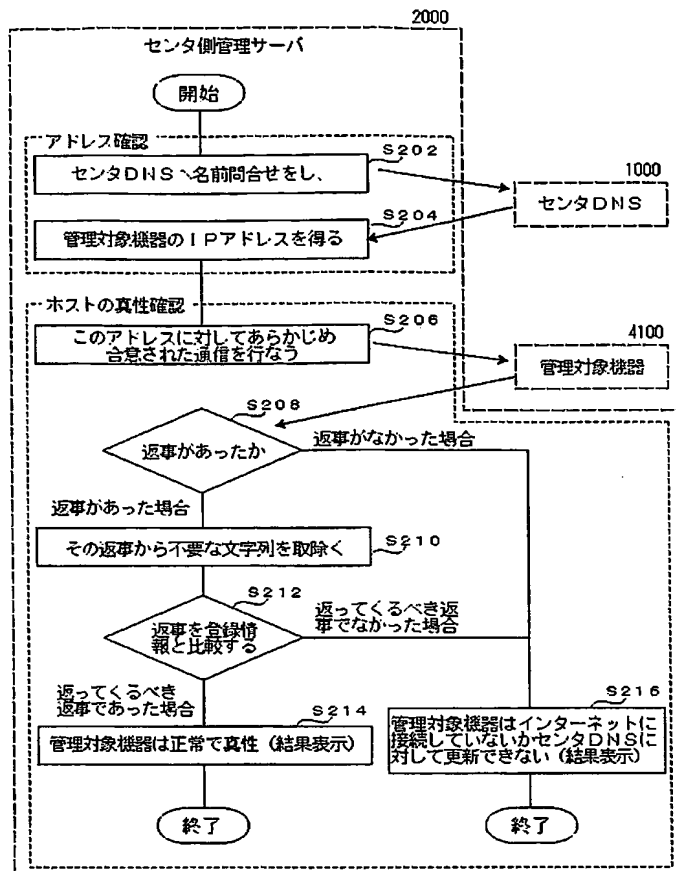

16
Fri Sep 13 00:00:39 JST 2002
result of DIG :218.218.1.188
PING bsdguru.dyndns.org (218.218.1.188): 56 data bytes
64 bytes from 218.218.1.188: icmp_seq=0 ttl=52 time=111.375 ms
64 bytes from 218.218.1.188: icmp_seq=1 ttl=52 time=117.394 ms

--- bsdguru.dyndns.org ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 111.375/114.385/117.394/3.010 ms

```

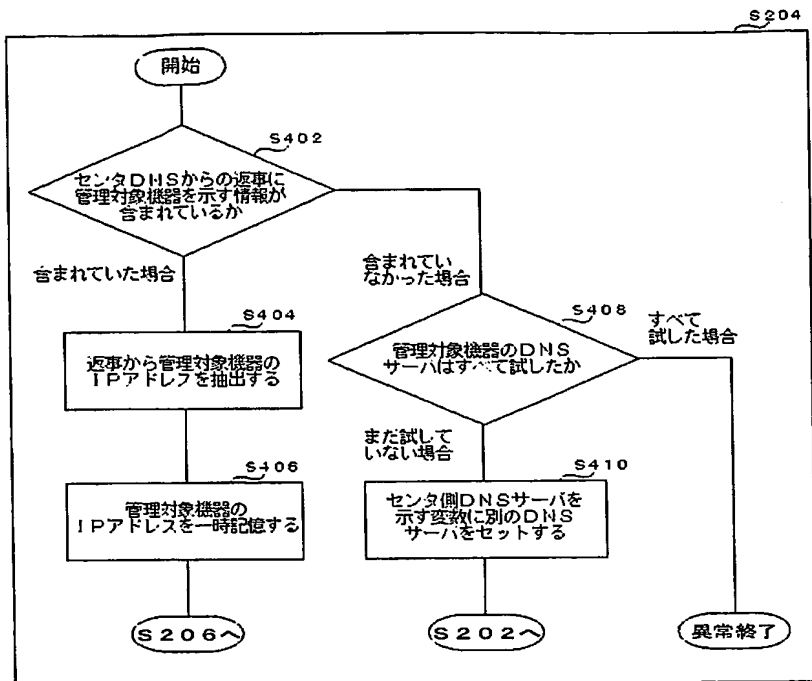
【図 27】

【図 27】



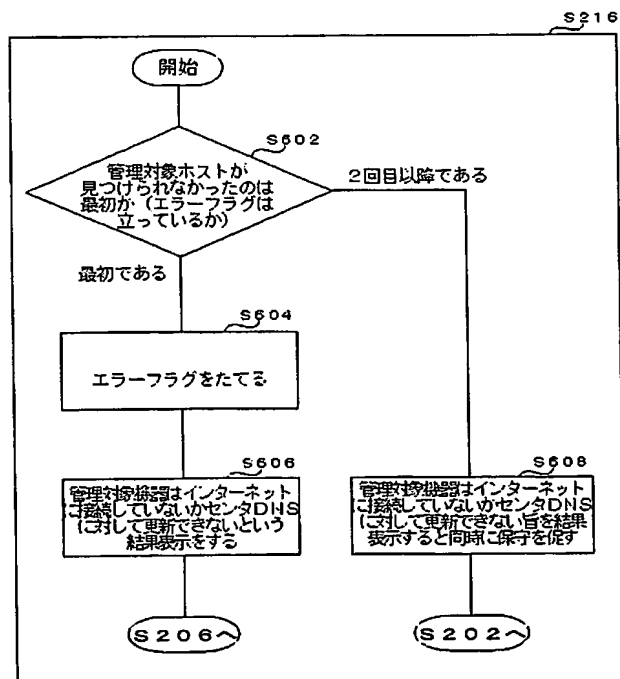
【図 28】

【図 28】



【図 29】

【図 29】



## 【図 30】

【図 30】

```

#!/bin/sh
### check! ##### set THIS
# Target host (FQDN)
DYNHOST=bsduru.dyndns.org
# Center DNS (FQDN)
[AC=asl.dyndns.org
#####
PATH=/bin:/usr/bin:/usr/local/bin:/sbin:/usr/sbin
ERRFLAG=/tmp/ERR.$DYNHOST

MSGDSP() { echo "date '+%Y/%m/%d %H:%M:%S'" "$@" ;}

DMSVAL=$(dig @$DMS $DYNHOST | grep $DYNHOST | grep "IN A" | cut -f4)
HOST01_CUR_lmp=$(nslookup $DMSVAL public systen.systame.0 ---)
|| ($STATUS=$? ; echo $STATUS)
HOST01_CUR=$(echo $HOST01_CUR_lmp | sed 's/system.systame.0 = //' )
if [ $DYNHOST != $HOST01_CUR ]; then
  if [ -f $ERRFLAG ]; then
    MSGDSP "EMERGENCY $0 : V"$DYNHOST" is missing at $HOST01_CUR"
  else
    touch $ERRFLAG
    MSGDSP "ABEND $0 : V"$DYNHOST" is missing at $HOST01_CUR"
  fi
  exit 1
fi
MSGDSP "OK $0 : V"$DYNHOST" is ALIVE at $DMSVAL"

rm -f $ERRFLAG
exit

```

## 【図 31】

【図 31】

2002/09/13 23:18:23 OK check!.sh : "bsduru.dyndns.org" is ALIVE at 218.218.1.188

## 【図 32】

【図 32】

(A)

2002/09/13 23:05:00 ABEND check!.sh : "bsduru.dyndns.org" is missing at 1

(B)

2002/09/13 23:05:00 ABEND check!.sh : "bsduru.dyndns.org" is missing at naka.koral.or.jp

## 【図 33】

【図 33】

(A)

2002/09/13 23:05:03 EMERGENCY check!.sh : "bsduru.dyndns.org" is missing at 1

(B)

2002/09/13 23:05:03 EMERGENCY check!.sh : "bsduru.dyndns.org" is missing at naka.koral.or.jp

## 【図 3 4】

【図 3 4】

```
% dig @ns1.dyndns.org bsdguru.dyndns.org

;<> DIG 8.3 <> @ns1.dyndns.org bsdguru.dyndns.org
; (1 server found)
;; res options: Inlt recurs defnaw dnsrcb
;; got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 8
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 5, ADDITIONAL: 5
;; QUERY SECTION:
;;      bsdguru.dyndns.org, type = A, class = IN

;; ANSWER SECTION:
bsdguru.dyndns.org.      IN IN A      218.48.105.100

;; AUTHORITY SECTION:
dyndns.org.             ID IN NS      ns4.dyndns.org.
dyndns.org.             ID IN NS      ns5.dyndns.org.
dyndns.org.             ID IN NS      ns1.dyndns.org.
dyndns.org.             ID IN NS      ns2.dyndns.org.
dyndns.org.             ID IN NS      ns3.dyndns.org.

;; ADDITIONAL SECTION:
ns1.dyndns.org.         ID IN A      66.37.215.43
ns2.dyndns.org.         ID IN A      209.89.32.137
ns3.dyndns.org.         ID IN A      64.71.191.26
ns4.dyndns.org.         ID IN A      212.100.224.171
ns5.dyndns.org.         ID IN A      66.37.215.44

;; Total query time: 231 msec
;; FROM: open-nases4commerce.net to SERVER: ns1.dyndns.org 66.37.215.43
;; WHEN: Fri Sep 13 23:24:31 2002
;; MSG SIZE sent: 86 rcvd: 222
```

## 【図 3 5】

【図 3 5】

```
% dig @hth.dyndns.org bsdguru.dyndns.org

;<> DIG 8.3 <> @hth.dyndns.org bsdguru.dyndns.org
; (1 server found)
;; res options: Inlt recurs defnaw dnsrcb
;; res_send to server hth.dyndns.org 66.189.169.16: Operation timed out
% echo $status
8
```

エラー出力

## 【図 36】

【図 36】

```
% dig @ns1.dyndns.org bsd2guru.dyndns.org

;<<> DIG 0.3 <> @ns1.dyndns.org bsd2guru.dyndns.org
; (1 server found)
;; res options: init recurs defname dnsrcb
;; got answer:
;; -->HEADER<-- opcode: QUERY, status: NXDOMAIN, id: 6
;; flags: qr aa rd: QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0
;; QUERY SECTION:
;;      bsd2guru.dyndns.org, type = A, class = IN

;; AUTHORITY SECTION:
dyndns.org.      10M IN SOA      ns1.dyndns.org. hostmaster.dyndns.org. (
                                2057408667      ; serial
                                10M      ; refresh
                                5M      ; retry
                                1W      ; expiry
                                10M )    ; minimum

;; Total query time: 215 msec
;; FROM: open.names4commerce.net to SERVER: ns1.dyndns.org 68.37.215.43
;; WHEN: Thu Sep 26 22:58:13 2002
;; MSG SIZE sent: 97 rcvd: 88

% echo $status
0
```

## 【図 37】

【図 37】

```
% snmpget 218.48.105.100 public system.sysName.0
system.sysName.0 = bsd2guru.dyndns.org
% echo $status
0
```

## 【図 38】

【図 38】

```
% snmpget 218.48.105.101 public system.sysName.0
Timeout: No Response from 218.48.105.101. エラー出力
% echo $status
1
```

## 【図 39】

【図 39】

```
% snmpget 218.48.105.100 wrongcommunity system.sysName.0
Error in packet
Reason: (noSuchName) There is no such variable name in this MIB.
Failed object: system.sysName.0 エラー出力
% echo $status
2
```

## 【図 40】

【図 40】

```
% snmpget 218.48.105.100 public system.sysLocation.0
system.sysLocation.0 = TEXT
% echo $status
0
```

## 【図 4 1】

【図 4 1】

```
options {
    directory "/etc/namedb";
    // forward only;
    forwarders {
        127.0.0.1;
    };
    version "Hyper-Returner-BOX";
    // query-source address * port 53;
    // dump-file "s/named_dump.db";
};
```

## 【図 4 2】

【図 4 2】

```
% dig @218.48.105.100 txt chaos version.bind

;<<> DIG 8.3 <<> 218.48.105.100 txt chaos version.bind
; (1 server found)
;; res options: init recurs defnau dnsrcb
;; got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 8
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUERY SECTION:
;;      version.bind, type = TXT, class = CHAOS

;; ANSWER SECTION:
VERSION.BIND.      0S CHAOS TXT      "Hyper-Returner-BOX"

;; Total query time: 78 msec
;; FROM: open.names4commerce.net to SERVER: 218.48.105.100
;; WHEN: Thu Sep 28 22:37:43 2002
;; MSG SIZE  sent: 30  rcvd: 73

% echo $status
0
```

## 【図 4 3】

【図 4 3】

```
% dig @218.48.105.101 txt chaos version.bind

;<<> DIG 8.3 <<> 218.48.105.101 txt chaos version.bind
; (1 server found)
;; res options: init recurs defnau dnsrcb
;; res_send to server 218.48.105.101: Operation timed out エラー出力
% echo $status
8
```

## 【図 4 4】

【図 4 4】

```
% dig @ns.koral.or.jp txt chaos version.bind

;<> DIG 0.3 <> @ns.koral.or.jp txt chaos version.bind
; (1 server found)
;; res options: init recurs defnam dnstch
;; got answer:
;; --HEADER-- opcode: QUERY, status: NOERROR, id: 8
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUERY SECTION:
;;      version.bind, type = TXT, class = CHAOS

;; ANSWER SECTION:
VERSION.BIND.      IN CHAOS TXT      "4.9.7-REL"

;; Total query time: 2 msec
;; FROM: open.names4commerce.net to SERVER: ns.koral.or.jp 202.217.175.5
;; WHEN: Thu Sep 26 22:40:57 2002
;; MSG SIZE sent: 80 rcvd: 84

% echo $status
0
```

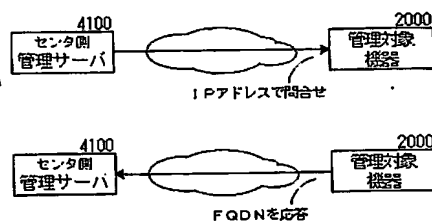
## 【図 4 5】

【図 4 5】

```
Trying 202.217.175.5...
Connected to ns.koral.or.jp.
Escape character is '^['.
220 ns.koral.or.jp ESMTP Sendmail 8.8.8/3.89-98062802; Tue, 5 Nov 2002 02:14:35
+0900 (JST)
```

## 【図 4 6】

【図 4 6】





【図 47】

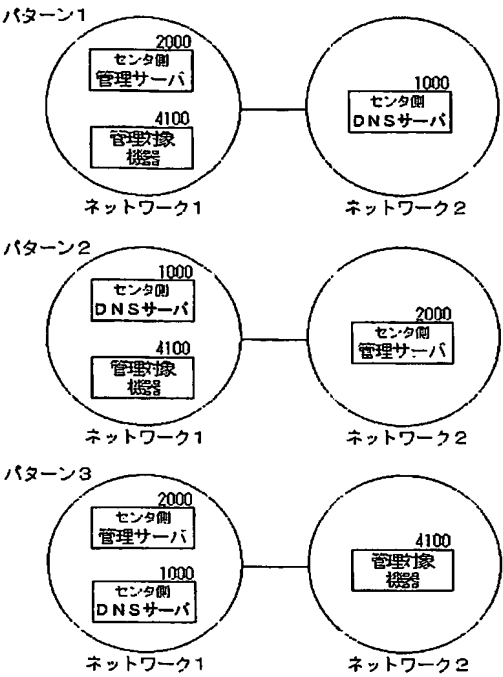
【図47】

実施例	管理対象装置	管理サーバ(200)		管理対象装置(100)
		サイン	カウンタースサイン#	
実施例1	管理対象装置	通信方式	合意された記事	＜－ カウンタースサイン（＜サイン）に於いての応答として検定する） （署名生成装置で署名生成）
	管理対象装置	通信方式	合意された記事	＜－ 合意された記事（＜サイン）に於いての応答として検定する） （署名生成装置で署名生成）
	管理対象装置	サイン	カウンタースサイン	＜－ カウンタースサイン（＜サイン）に於いての応答として検定する）
実施例2 ないし 実施例8	管理対象装置	通信方式	合意された記事	＜－ 合意された記事（＜サイン）に於いての応答として検定する）
	管理対象装置	サイン	カウンタースサイン	＜－ カウンタースサイン（＜サイン）に於いての応答として検定する）
	管理対象装置	通信方式	合意された記事	＜－ 合意された記事（＜サイン）に於いての応答として検定する）
実施例9	管理対象装置	サイン	カウンタースサイン （＝FODN）	＜－ カウンタースサイン（＜サイン）に於いての応答として検定する） （署名生成装置で署名生成）
	管理対象装置	通信方式	合意された記事 （＝FODN）	＜－ 合意された記事（＜サイン）に於いての応答として検定する） （署名生成装置で署名生成）
	管理対象装置	サイン	カウンタースサイン	＜－ カウンタースサイン（＜サイン）に於いての応答として検定する）
実施例10	管理対象装置	サイン	カウンタースサイン	＜－ カウンタースサイン（＜サイン）に於いての応答として検定する）
	管理対象装置	通信方式	合意された記事	＜－ 合意された記事（＜サイン）に於いての応答として検定する）
	管理対象装置	サイン	カウンタースサイン	＜－ カウンタースサイン（＜サイン）に於いての応答として検定する）

※ 管理サーバ(200)に設定される管理対象装置名がFODNである場合、検定不要。  
管理サーバ(200)に設定される管理対象装置名がFODNでない場合は、FODNを検定する。

【図48】

【図48】



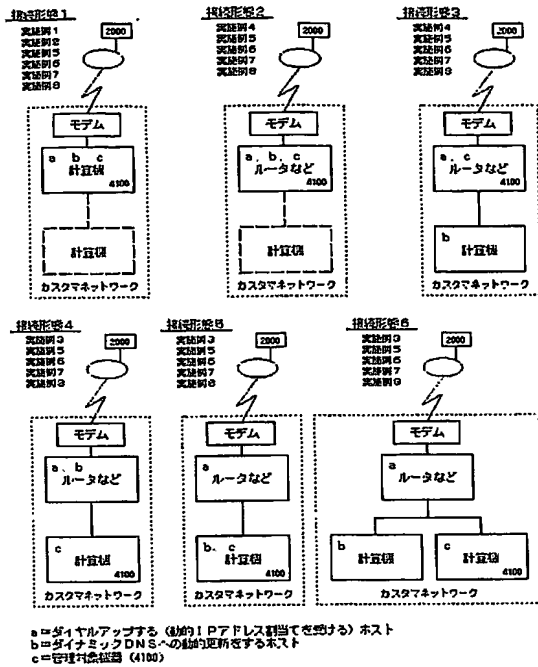
【図49】

【図49】

	WAN	DNS	インターネットによる到達性	ネットワーク上の到達性	インターネット上の到達性
インターネットに接続する事業者が接続されない、広域の網の境目	①	公共	WAN網上であり	接続するネットワーク上の到達性	接続するネットワーク上の到達性
	②			2つ以上 (LAN-WAN)	2つ以上 (LAN-WAN)
	③			WAN網上であり	2つ以上 (LAN-WAN)
	④	私設		WAN網上であり	2つ以上 (LAN-WAN)
	⑤			あり	1つ (WANのみ)
LANのみの場合	⑥			2つ以上 (LAN-WAN)	2つ以上 (LAN-WAN)
	⑦	なし		あり	1つ (LANのみ)
	⑧			あり	2つ以上 (LAN-WAN)
	⑨			あり	2つ以上 (LAN-WAN)
	⑩			あり	2つ以上 (LAN-WAN)

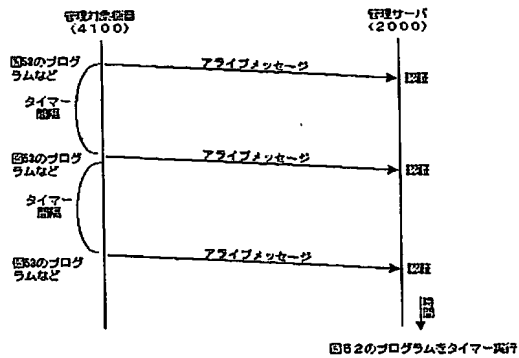
【図 50】

【図 50】



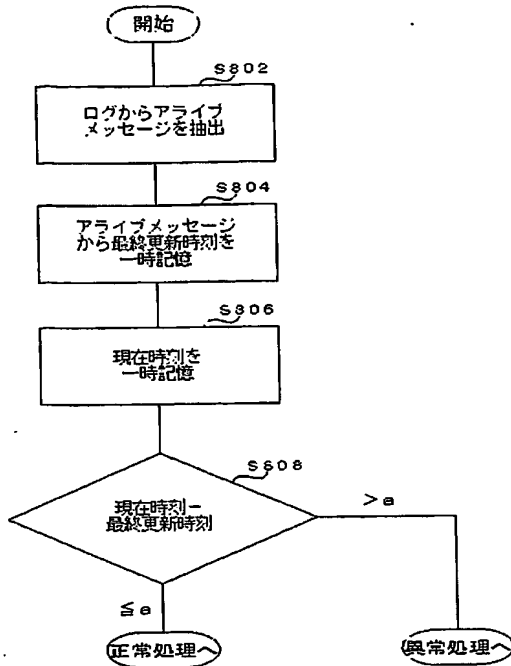
【図 51】

【図 51】



【図 5 2】

【図 5 2】



【図 5 3】

【図 5 3】

```

$1/bin/sh
ftp -n agr.center.names4commerce.com << EOF
user hbuser01 hbuser01
etelus
bye
EOF
    
```

【図 5 4】

【図 5 4】

```

Sep 10 21:04:19 agr f1pd[20008]: connection from Tokyo-ppp06.korai.or.jp
Sep 10 21:04:19 agr f1pd[20008]: <--- 220
Sep 10 21:04:19 agr f1pd[20008]: agr.center.names4commerce.com FTP server (Version 8.00) ready.
Sep 10 21:04:19 agr f1pd[20008]: command: CYCT
Sep 10 21:04:19 agr f1pd[20008]: <--- 215
Sep 10 21:04:19 agr f1pd[20008]: UNIX Type: L8 Version: BSD-199008
Sep 10 21:04:19 agr f1pd[20008]: command: USER hbuser01
Sep 10 21:04:19 agr f1pd[20008]: <--- 331
Sep 10 21:04:19 agr f1pd[20008]: Password required for hbuser01.
Sep 10 21:04:19 agr f1pd[20008]: command: PASS ???
Sep 10 21:04:19 agr f1pd[20008]: <--- 230
Sep 10 21:04:19 agr f1pd[20008]: User hbuser01 logged in.
Sep 10 21:04:19 agr f1pd[20008]: FTP LOGIN FROM Tokyo-ppp06.korai.or.jp as hbuser01
Sep 10 21:04:19 agr f1pd[20008]: command: QUIT
Sep 10 21:04:19 agr f1pd[20008]: <--- 221
Sep 10 21:04:19 agr f1pd[20008]: Goodbye.
    
```

【図 5 5】

【図 5 5】

```

Sep 23 19:39:15 test f1pd[554]: connection from Tokyo-ppp06.korai.or.jp (202.217.176.101)
Sep 23 19:39:15 test f1pd[554]: FTP LOGIN FAILED FROM Tokyo-ppp06.korai.or.jp, hbuser01
    
```



【書類名】 要約書

【要約】

【課題】 固定的な IP アドレスを与えられた TCP/IP ネットワーク上のホストの管理は、通常であれば機器監視として ping コマンドなどを利用してホストの活死を監視することができる。しかしダイヤルアップのホストにあっては、その IP アドレスが変化することから、管理対象ホストでないホストが ping に応えていても管理対象機器は稼動していることになってしまい、管理できない。動的 IP アドレスの機器を管理する基本的なメカニズムを提供する。

【解決手段】 サイン・アンド・カウンターサインを用いて、動的に IP アドレスが変化するホストの活死確認および真性を確認する。また、通常の間管理をおこなう場合にも、従来であれば IP アドレスが変化するホストは管理することができなかったが、通常の間管理の前段の処理として本発明を用いることによって、その後のより高度な管理（例えば、CPU 負荷やネットワークトラフィックの監視）をも可能とした。

【選択図】 図 13

## 認定・付加情報

特許出願の番号	特願 2002-371448
受付番号	50201944068
書類名	特許願
担当官	大竹 仁美 4128
作成日	平成15年 1月 7日

## &lt;認定情報・付加情報&gt;

【提出日】	平成14年12月24日
【特許出願人】	申請人
【識別番号】	300062120
【住所又は居所】	東京都中野区野方二丁目6番3号
【氏名又は名称】	有限会社グルーネット
【特許出願人】	
【識別番号】	301047980
【住所又は居所】	東京都中野区野方二丁目6番3号
【氏名又は名称】	福島 一

次頁無

【書類名】 出願人名義変更届  
【整理番号】 P021224NSC  
【提出日】 平成15年12月 4日  
【あて先】 特許庁長官殿  
【事件の表示】  
【出願番号】 特願2002-371448  
【承継人】  
【識別番号】 301047980  
【氏名又は名称】 福島 一  
【譲渡人】  
【識別番号】 300062120  
【氏名又は名称】 有限会社グルーネット  
【代表者】 福島 一  
【手数料の表示】  
【予納台帳番号】 212050  
【納付金額】 4,200円  
【その他】 本件は、譲渡人有限会社グルーネットの持分放棄による承継人福島一への持分移転である。  
【提出物件の目録】  
【物件名】 持分放棄証書 1  
【援用の表示】 特願 2 0 0 2 - 3 7 1 4 4 8 の出願人名義変更届に添付のものを援用する。



特願 2002-371448

出願人履歴情報

識別番号

[300062120]

1. 変更年月日

2000年 8月 5日

[変更理由]

新規登録

住 所

東京都中野区野方二丁目62番3号

氏 名

有限会社グルーネット

特願 2002-371448

出願人履歴情報

識別番号

[301047980]

1. 変更年月日

2001年 7月12日

[変更理由]

新規登録

住 所

東京都中野区野方二丁目62番3号

氏 名

福島 一